There is currently intense interest in robotic and autonomous systems, both in the technical and engineering communities and more broadly. These systems have always been appealing as they blend social impact, technology, science fiction, and philosophy with newsworthy speculation and sensationalism in imagined futures. These futures might arrive much faster than we thought as technology (sensors, actuators, power, and sensing and learning) converges with strong business drivers and social need. The diverse applications include, inter alia, green mobility (just summon a car-pod to take you to see friends or shops), healthcare robots to serve an aging population, robotic surgery, autonomous freight deliveries, safe and greener motorway driving, and post-accident work in hazardous and uncertain nuclear environments.

A spectrum of systems falls under the “autonomy” umbrella, from incremental improvements to existing automation assistance to fully autonomous future systems. The US National Airspace System’s (NAS’s) 2014 study Autonomy Research for Civil Aviation: Toward a New Era of Flight coined the phrase “increasingly autonomous” (IA) systems and identified assurance as the one critical, cross-cutting challenge. After a detailed examination of the issues, it identified four major barriers to ensuring that IA systems will enhance rather than diminish NAS’s safety and reliability:

- certification process,
- decision making by adaptive/nondeterministic systems,
- trust in adaptive/nondeterministic IA systems, and
- verification and validation.

Addressing the assurance of IA and fully autonomous system challenges will require a multidisciplinary approach with social and political engagement, as these systems’ risks and resilience—or what we would like from them—are by no means clear. As usual, some will reap the benefits and some will suffer the risks, and this division might not be fair. We will probably be more vulnerable to widespread chaos and confusion. How we deal with this and who pays for the systems that recover the situation must be debated. (As we know, markets can drive out resilience unless incentives or regulations are explicitly designed to prevent this.)

Although these autonomous systems will be part of ultra large systems of systems with complex system behavior and will adapt to success, failure, social changes, and political interaction, they must still be engineered to be trustworthy. When I see the certification and assessment effort that goes into a simple device in the nuclear, rail, and aerospace industries, the task of assuring autonomous systems seems daunting.

However, we know that we need appropriate system architectures and trusted components. We need architectures that limit parts of the system that must be highly trusted, building on current ideas of protection systems with static safety envelopes to more dynamic, real-time evaluation of safety invariants based on deeper system properties. These can be thought of—rather fancifully—as prototypical explicit ethical systems in an autonomous systems architecture that can be assured. So, we seek ethical behaviors, some of which will be rule based while others will be an emergent property of the complex and complicated systems and associated software.

Cyber and security issues are enormously challenging. Recent well-publicized car hacking incidents show the risks of not addressing these facets in current systems, let alone future ones. As Terry Benzel discussed in the last IEEE Security & Privacy issue, there’s an ongoing discussion of cyber-related research strategies. This, as well as the updates to the UK strategy that are being discussed now and
will lead to a refresh in 2106, should address the challenges and benefits of autonomy head-on—both because it’s a strategic objective, important in its own right, and because addressing it will pull through technologies and insights that can be deployed from existing automation to fully autonomous systems.

Research and innovation to address the “assurance gap” should examine the basic principles behind assurance to see whether they’re applicable to autonomous systems and what insights a return to basic principles could bring. Recently, I’ve been involved in several initiatives to distill the safety principles for automation systems in the nuclear industry, drawing on the work of the International Atomic Energy Agency and the UK Safety Assessment Principles. This has led to the following principles:

1. Effective understanding of the hazards and their control should be demonstrated.
2. Intended and unintended behavior of the technology should be understood.
3. Multiple and complex interactions between technical systems as well as human systems to create adverse consequences should be recognized.
4. Active challenge should be part of decision making throughout the organization. All stakeholder needs should be accounted for to understand and challenge the case in its structure and presentation.
5. Lessons learned from internal and external sources should be incorporated.
6. Justification should be logical, coherent, traceable, accessible, and repeatable with a rigor commensurate with the system’s required degree of trust.

Can we apply these principles to autonomous systems? It’s interesting that their emphasis on understanding, explanation, challenge, and learning are quite general and raises the question of who, or what, should have this understanding. So, as we reinvent our approach to assurance, perhaps we should shift from thinking of the dependability of these systems as complex automatic gadgets (for instance, how we can apply DO178C or IEC 61508 to them) to whether and how their assurance addresses the principles of understanding, explanation, challenge, and learning.

In addition, we might get more leverage by taking an anthropomorphic viewpoint—whether as a metaphor or quite literally. In the UK, as in many other countries, an individual has to pass only a single practical driving test and an additional theory exam on the rules to drive a car. This might take 25 to 30 hours of driving lessons. Flying a private plane requires 70 (www.aopa.org/letsgo flying/faqs.html). This would seem sufficient to take an individual from almost certain failure to a socially acceptable rate of self-harm.

In simple architectural terms, we can think of this in the usual specific application versus generic platform distinction. One reason we trust the human “platform” is because we assume some built-in characteristics of self-preservation and learned ethics. In addition, there’s evidence that humans can do “similar” or more difficult tasks than autonomous systems, for instance, walk, ride a horse, ride a bicycle, or cross the street in a rush hour—and we have evidence, or a belief, that the abilities required are quite generic. If we have a less trustworthy platform then we require more specific evidence: my blind friend trusts his safety to his guide dog as he commutes into London, but the specific training took far longer than would be required from a human helper. So, fully autonomous systems will be easier to assure and license once they have a trusted and widely used platform.
We might see several tipping points or transitions in assurance, the market, and uptake. The first concerns assurance, when automation becomes too complex to assure unless it’s based on a self-adaptive, explanatory understanding. The second is that, as with PC operating systems in the 1990s, whoever owns the trustworthy platform will dominate the industry. The third is in risk behavior in which the use of an autonomous vehicle is the norm and nonuse must be justified. Finally, when we give autonomous vehicles only a simple driving test, as we do with teenagers, we will know that trust in autonomous transport has really arrived.

References

The Department of Computer Science at Virginia Tech (www.cs.vt.edu) seeks applicants for tenure-track faculty positions in three areas: interactive computing, cyber security, and data analytics. Candidates should have a Ph.D. in Computer Science or related field at the time of appointment, a rank-appropriate record of scholarship and collaboration in computing and interdisciplinary areas, sensitivity to issues of diversity in the campus community, and will be required to teach at the undergraduate and/or graduate levels. The position requires occasional travel to professional conferences and meetings.

Tenure-track Assistant Professor in Interactive Computing – Blacksburg, VA
Strong candidates from any area related to interactive computing are encouraged to apply. Exceptional candidates at higher ranks will also be considered. Candidates who complement existing strengths in human-computer interaction, graphics, intelligent user interfaces, visualization, visual analytics, human interaction with big data, augmented reality, tangible interfaces, human-robot interaction, game design, creativity support, or computing in the arts and humanities are especially encouraged. Candidates have opportunities for collaboration in the interdisciplinary Center for Human-Computer Interaction (cici.cs.vt.edu) and the Institute for Creativity, Arts, and Technology (icat.vt.edu) housed in the new Moss Center for the Arts, and the Discovery Analytics Center (dac.cs.vt.edu). Applications must be submitted online to http://jobs.vt.edu for posting #TR0150108. Inquiries should be directed to Dr. Chris North, Search Committee Chair, north@vt.edu.

Tenure-track Assistant Professor in Cyber Security – Blacksburg, VA
Candidates with expertise in cyber security, including technologies for and applications in information security, network security, and trustworthy computing are encouraged to apply. Candidates focusing on security issues of cyber-physical systems, embedded systems, sensor networks, robotics, Internet of Things (IoT), etc. are especially encouraged. The candidate will join the CS department and also participate in an interdisciplinary team of five faculty in Advanced Manufacturing and share common space and equipment, leveraging established labs and the Commonwealth Center for Advanced Manufacturing (www.ccamb-va.com/), a public-private partnership in Virginia. There is an active group of cyber security faculty in CS and ECE departments collaborating in research as well as graduate and undergraduate education (see: www.cyber.vt.edu). Applications must be submitted online to http://jobs.vt.edu for posting #TR0150107. Inquiries should be directed to Dr. Ali Butt, Search Committee Chair, butta@cs.vt.edu.

Associate/Full Professor in Data Analytics – National Capital Region (NCR)
Candidates with research depth and breadth in data analytics, data mining, “big data”, or data science are encouraged to apply. Candidates working at the intersection of data analytics and cyber-security and at the intersection of data analytics and urban computing are especially encouraged. Candidates should present a proven ability to initiate and sustain collaborations within computing as well as with application specialists. The department is home to the Discovery Analytics Center (dac.cs.vt.edu) that leads “big data” research on campus. The successful candidate will contribute to the research and graduate programs in the NCR and collaborate with faculty at Virginia Tech’s campus in Blacksburg, VA. The NCR campus (www.ncr.vt.edu) is located near the Washington D.C./Falls Church area and houses the Virginia Tech Research Center (www.nrc.vt.edu/arlington) in Arlington, VA. Applications must be submitted online to http://jobs.vt.edu for posting #TR0150106. Inquiries should be directed to Dr. Naren Ramakrishnan, Search Committee Chair, naren@cs.vt.edu.

The Department of Computer Science has 40 research oriented tenure-track faculty and ~10 postdocs/research faculty. There are a total 12 NSF/DOE CAREER awardees in the department. Research expenditures for FY2015 were $412 thousand per tenure-track faculty member (i.e., a total of $15.5 million); total research funding at the beginning of FY2015 was $43.4 million. BS, MS, and PhD degrees are offered, with a growing enrollment of over 610 undergraduate majors (14% women) and over 270 PhD/MS students. In 2010, CS@VT was ranked 5th in the country in recruiting quality of CS undergrads by the Wall Street Journal. The department is in the College of Engineering, whose undergraduate program was ranked 8th and graduate program was ranked 12th among public engineering schools in 2014 by U.S. News & World Report.

Early applications are encouraged. We welcome applications from women or minorities. Salary for suitably qualified applicants is competitive and commensurate with experience. Selected candidates must pass a criminal background check prior to employment.

Virginia Tech is an AA/EEO employer; applications from members of underrepresented groups are especially encouraged.