Academic Corner
Hang Su

In this issue, we interview IEEE SMC member Dr. Francesco Flammini. He has been a Professor of Computer Science with a focus on trustworthy autonomous systems at the University of Florence (Italy), University of Applied Sciences and Arts of Southern Switzerland, Mälardalen University, and Linnaeus University (Sweden). Previously, he spent 15 years in industry, working on intelligent transportation, critical infrastructure protection, and cybersecurity for organizations such as Ansaldo STS (now Hitachi Rail) and IPZS. Flammini has led several research groups, study programs, and numerous international research projects, particularly in AI for smart railways. He is a Senior Member of IEEE, Associate Vice-President for Members and Student Activities of the IEEE SMC Society, and Chair of its Homeland Security Technical Committee. He is also a Distinguished Visitor of the IEEE Computer Society and a Distinguished Lecturer of ACM. He has authored 150+ technical publications and served as a chair, editor, and reviewer for leading conferences and journals. He has been a principal investigator in 15+ EU-funded projects and supervised over 10 PhD students. His work has earned multiple awards, including the Dalle Molle Award for Quality of Life (2024), the Transport Research Arena Senior Researcher Award (2024), and inclusion in Stanford's Top 2% Scientists list (2023). Dr. Flammini serves as an Associate Editor for the IEEE Transactions on Emerging Topics in Computing and other prestigious journals.

(1) What inspired you to follow your research direction?
I have been fortunate to experience two professional paths—one in industry and one in academia, the latter of which is still ongoing. My career began in a large company developing transportation systems, where I was hired as a software engineer primarily responsible for the verification and validation of real-time control systems. At the same time, in the fall of 2003, I began my PhD in Computer Engineering at the University of Naples Federico II, where I had also earned my five-year master's degree. Despite balancing work and studies, I completed my PhD in just three years—a rare achievement for student-workers.

Following my PhD, I took on leadership roles in innovation projects, mainly funded by the European Union, with a focus on the safety and security of critical infrastructure. This phase of my career lasted nearly 15 years, during which I received several international innovation awards in my field, particularly in railway transportation. Meanwhile, I remained actively engaged in research, publishing papers and books, and serving as an adjunct professor at various universities.

I also spent a few years working at the Italian State Mint and Polygraphic Institute—the state-owned company responsible for security printing of coins, passports, and other sensitive materials—where I was hired as an information security and compliance manager. However, I eventually felt a growing desire to return more fully to research and teaching. This led me to transition to academia full-time. I began as a senior lecturer and quickly advanced to full professor, where I now lead research groups and projects and supervise PhD students.

My industrial background has been invaluable in building strong connections with companies and securing external funding. Additionally, as a chartered professional engineer, I have worked as a technical consultant, particularly for the judiciary in litigation cases involving software systems. This role has allowed me to remain actively engaged in the engineering profession, which I consider essential.

(2) What are some of the key challenges in cyber-physical systems and industrial cybersecurity today?
I often say that the combination of complexity and criticality represents the greatest challenge for cyber-physical systems (CPS). Complexity arises from factors such as size, distribution, and heterogeneity, constantly increasing when considering simple metrics like lines of code, as well as broader aspects like ubiquitous and pervasive computing, enabled by the Internet of Things and edge-cloud paradigms. Criticality, on the other hand, relates to the potential consequences of threats to CPS, which can range from significant financial losses to the loss of human lives. These factors make industrial cybersecurity particularly difficult to

ensure, as risk assessments must account for a wide array of considerations, including strategic and adversarial attacks on artificial intelligence and machine learning systems—an emerging and growing phenomenon.

(3) How do you envision the future of cybersecurity, AI-driven safety, and critical infrastructure protection in the next 5–10 years?
To put it simply, we can distinguish between "AI for security" and "Security for AI." I use the term security as a simplification, as this concept encompasses all dependability attributes, including reliability and safety.

"AI for security" refers to the use of advanced situational awareness, decision support systems, and AI-based threat and anomaly detection, leveraging both supervised and unsupervised learning approaches. These methods have become essential in helping humans recognize and manage complex threat scenarios, particularly in the evolving landscape of cyber warfare—a growing concern due to recent socio-political tensions and ongoing conflicts.

Conversely, "Security for AI" focuses on addressing the risks and emerging threats associated with machine learning systems, such as opacity, bias, data poisoning, and adversarial attacks. While AI holds immense potential for enhancing security, it also introduces vulnerabilities that can be exploited by attackers. These two perspectives - AI strengthening security and security safeguarding AI - are two sides of the same coin, presenting numerous challenges that will need to be addressed.

(4) What advice would you give to young researchers aspiring to contribute to these fields?
I supervise several young researchers working on topics related to trustworthy AI and explainability. When I was a young researcher working with critical systems, having expertise in reliability theory, stochastic modeling, dependable computing, fault tolerance, software engineering, and formal methods was sufficient to gain a comprehensive understanding of the state of the art. Today, however, the landscape has become significantly more complex, requiring young researchers to develop a much broader background that now includes machine learning and autonomous robotics—disciplines that demand considerable effort to master.

Since no one can be an expert in everything, one of the biggest challenges—especially at the beginning of a PhD journey—is selecting the right topics to study to address a given research question. I usually recommend starting with a systematic literature review and focusing on industry-relevant challenges. This approach helps researchers navigate the field more easily and converge on a manageable research direction that fits within the constraints of limited resources and time while still producing significant and industrially exploitable results.

To manage complexity, I suggest beginning with a simple case study and developing a proof of concept within a reasonable timeframe. Complexity can then be gradually increased step by step to ensure significance and scalability of the research for real-world applications. Being an engineer before a professor, my primary focus is on applied research. As a result, highly abstract findings with a long-term exploitation horizon are not my main area of interest. Instead, I emphasize research that can deliver practical, impactful solutions.

(5) How has IEEE influenced your professional journey?
I believe IEEE has had a profound influence on my professional journey. I joined IEEE as a PhD student, taking advantage of the special student discounts. Early on, I started receiving review requests from top journals, such as IEEE Transactions on Computers. Reading those papers, I learned a great deal—and at times, I even doubted whether I would ever be able to write a paper of such high quality. Fortunately, time proved me wrong. This experience motivated me to invest a significant amount of time as a young researcher serving as a peer reviewer. I am not sure whether students today fully recognize the importance of reading high-quality papers—not only to gain knowledge but also to identify potential weaknesses in reasoning. For me, it was truly a privilege. After a few years, I took on leadership roles in local IEEE units and technical committees—first within the Computer Society and later in the Systems, Man, and Cybernetics Society. Today, I serve on the Board of Governors as the Associate Vice President for Student and Member Activities (MSA). Now, my privilege extends beyond personal growth; I have the opportunity to support and shape IEEE's strategic direction through the SMC Society and its valuable initiatives.