Defence Research and Development Canada
Recherche et développement pour la défense Canada

Cybersecurity for Critical Systems

Literature Survey

Brenda Brady
National Research Council Institute for Scientific and Technical Information

Prepared by:
National Research Council Institute for Scientific and Technical Information
1200 Montreal Road, Building M-55
Ottawa, Ontario
Canada K1A 0R6

Contractor's document number: STI Assessment 14926
Contract project manager: Brenda Brady, 902-367-7552
PWGSC contract number: SRE07-001-033
CSA: François Bernier, Defence scientist, 418-844-4000 x4346

Defence Research and Development Canada – Valcartier

Contract Report
DRDC Valcartier CR 2013-188
June 2013

Canada

Cybersecurity for Critical Systems

Literature Survey

Brenda Brady
National Research Council Institute for Scientific and Technical Information

Prepared by:
National Research Council Institute for Scientific and Technical Information
1200 Montreal Road, Building M-55
Ottawa, Ontario
Canada K1A 0R6

Contractor's document number: STI Assessment 14926
Contract project manager: Brenda Brady, 902-367-7552
PWGSC contract number: SRE07-001-033
CSA: François Bernier, Defence scientist, 418-844-4000 x4346

Defence Research and Development Canada – Valcartier

Contract Report

DRDC Valcartier CR 2013-188

June 2013

IMPORTANT INFORMATIVE STATEMENTS

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of the Department of National Defence of Canada.

Abstract

To assist Defence Research and Development Canada as it develops cybersecurity strategies for cyber-physical systems (CPS), NRC Knowledge Management conducted a literature survey and analysis of 2,220 publications drawn from scientific and technical databases. The survey found that research attention is gradually shifting from conventional approaches to cybersecurity, such as intrusion detection, to those that include a more holistic and integrated view of both cyber and physical aspects. Modeling and simulation play a key role in developing and testing security systems. Various CPS-specific modeling methods, such as those that incorporate state estimation or intelligent , interactive layers are also being explored.

Because of the criticality of most cyber-physical systems and their role in national security, many CPS modeling solutions specifically address safety, reliability and risk management; resilience and survivability are key.

Key players in CPS cybersecurity are U.S. academic institutions and government laboratories, but commercial enterprise is also active. Much of the current research is being driven by security needs of wireless sensor networks and electrical grids, but other sectors, such as the automotive industry, are also participants. Because innovations may first be seen and research partnerships may thrive in domains that are not overtly military, it is recommended that DRDC maintain a broad perspective white pursuing its own research goals for CPS cybersecurity.

Résumé

En vue de soutenir Recherche et développement pour la défense Canada (RDDC) dans l'élaboration d'une stratégie pour la sécurité des systèmes cyber-physiques (SCP), CNRC Gestion du savoir a effectué une analyse de 2220 notices bibliographiques extraites de la littérature scientifique et technique. L'étude a révélé que l'attention des chercheurs se déplace progressivement des approches traditionnelles de cybersécurité a une perspective plus holistique et intégrée des aspects cybers et physiques. La modélisation et la simulation jouent un rôle clé dans le développement et l'essai des systèmes de sécurité. Diverses méthodes de modélisation - spécifiques aux SCP sont à l'étude, y compris certaines intégrant l'estimation d'état, l'intelligence artificielle ou les couches interactives.

En raison de la nature essentielle de la plupart des systèmes cyber-physiques et de leur rôle dans la sécurité nationale, de nombreuses solutions de modélisation se penchent sur la sécurité, la fiabilité et la gestion des risques; la résilience et la survie sont considérées comme des qualités essentielles.

Les principaux joueurs du domaine de la sécurité des SCP sont des institutions universitaires et des laboratoires gouvernementaux américains, mais des entreprises commerciales sont également actives dans le secteur. Une grande partie de la recherche actuelle est motivée par les besoins de sécurité des réseaux de capteurs sans fil et des réseaux électriques, mais d'autres secteurs, comme l'industrie automobile, y participent également. Parce que les innovations peuvent d'abord être

vues et des partenariats de recherche peuvent se développer dans des domaines qui ne sont pas ouvertement militaires, il est recommande a RDDC de maintenir une perspective large dans la poursuite de ses propres objectifs de recherche en matière de cybersécurité pour les systèmes cyber-physiques.

Executive summary

Cybersecurity for Critical Systems: Literature Survey

Brenda Brady; DRDC Valcartier CR 2013-188; Defence Research and Development Canada – Valcartier; June 2013.

The intent of this project was to provide an overview of the state of the art of cyber-defence strategies for cyber-physical systems (CPS), including wireless sensor networks, embedded systems, and other complex systems which form part of critical infrastructures or mission-critical processes. Not only should cybersecurity strategies detect and react to individual or multiple threats, they should also enable resilience to or recovery from such attacks. In addition to characterizing the CPS cybersecurity environment, the project sought to understand how modeling and simulation may contribute to security solutions for CPS, in order to determine future research directions.

Evidence for the project was gathered by means of a literature search in scientific and technical databases and conference proceedings, supplemented by references provided by the client. Results were loaded into data mining software for generation of analyses and visualizations.

Insights and Recommendations

- The field of CPS cybersecurity is relatively new and growing. Much of the research is exploratory in nature, and it is just moving into niche areas, such as specific sectors.
- Research is currently being driven by large-scale CPS systems such as the smart grid and public utilities, many of which are critical to national security. Innovation may occur first here.
- Many of tomorrow's solutions may arise from environments which are not are overtly military in nature. Research partnerships may thrive in all of these application areas. Therefore, we recommend that DRDC maintain a broad focus when considering research directions for cybersecurity of critical systems.

Table 1 summarizes project findings pursuant to the key questions of the mandate.

Table 1. Key Findings

Issue	Findings
Cyber-physical Systems (CPS) Security	• **Network security**: conventional methods of network security such as authentication or intrusion detection have dominated research until recently. • **Research attention shifts**: security solutions are moving beyond conventional network security to consider more complex, integrated, and layered cyber-physical approaches. • **Safety, reliability, and risk management**: because of the criticality of CPS systems, safety, reliability, and risk management are key elements in security strategies. • **Modeling & simulation (M&S)**: growing numbers and more varied M&S applications are apparent in the literature. • **Sectors:** chiefly wireless sensor networks, smart grids and public works
CPS Emerging Topics	• Modeling and simulation • Hierarchical frameworks • Artificial Intelligence, agent-based, predictive techniques • Risk management • Real time models and response times
CPS Major Players	• Academic institutions in the United States are dominant, but considerable research is ongoing in China. Commercial players are also active, often collaborating with universities or government labs. • **Academic**: University of Illinois, Carnegie Mellon, University of California at Berkeley, Massachusetts Institute of Technology • **Commercial:** Électricité de France, CESI Ricerca (Milan), MITRE Corporation, SRI International • **Research & Technology Organizations**: Electronics & Telecommunications Research Institute (South Korea), Royal Institute of Technology (Sweden) • **Government**: Idaho and Sandia National Laboratories, National Institute of Standards and Technology • **Military**: Air Force Institute of Technology, Air Force Research Labs in NY and OH, National University of Defence Technology (China)
Modeling & Simulation (M&S) Major Topics	• Models or methods with particular CPS application: threat/defence, stochastic, Markov, formal methods • Hybrid, hierarchical, dynamic modeling environments • Contribution of M&S to safety and risk management: for example, software/system testbeds used to develop risk assessments
M&S Emerging Topics	• Resilience, reliability, safety, risk • Real time • Artificial intelligence/learning, predictive methods • Smart grid, but also other application areas, e.g., automotive

Issue	Findings
M&S Players	• More international participation is seen for M&S topics • Players generally mirror those for all CPS cybersecurity (above), with some exceptions: Texas A&M University, Missouri University of Science & Technology, Northwestern Polytechnic (China), Fraunhofer Institute (Germany)

This page intentionally left blank.

Sommaire

Cybersecurity for Critical Systems : Literature Survey

Brenda Brady ; DRDC Valcartier CR 2013-188 ; Recherche et développement pour la défense Canada – Valcartier ; juin 2013.

Le but de ce projet était de fournir une vue d'ensemble de l'état de l'art dans le domaine des stratégies de cyber-défense des systèmes cyber-physiques (SCP), y compris les réseaux de capteurs sans fil, les systèmes intégrés et d' autres systèmes complexes faisant partie des infrastructures critiques ou des processus essentiels aux missions militaires. Non seulement les stratégies de cyber-sécurité devraient-elles détecter et réagir aux menaces individuelles ou multiples, elles devraient également permettre la résilience ou la récupération après de telles attaques. En plus de la caractérisation du secteur de la cybersécurité, le projet visait à mieux comprendre comment la modélisation et la simulation peuvent contribuer à des solutions de sécurité pour les SCP. Cela permettra de déterminer les orientations futures de la recherche.

Les données pour le projet ont été recueillies au moyen de recherches dans des bases de données scientifiques et techniques ainsi que dans des comptes rendus de conférences. La recherche a étécompléte par des références fournies par le client. Les résultats ont été téléchargés dans un logiciel permettant de produire des analyses et des visualisations.

Aperçus et recommandations

- Le domaine de la cybersécurité des SCP est relativement nouveau et en pleine croissance. Une grande partie de la recherche est de nature exploratoire, et le domaine se déplace justement vers des zones de niche, comme des secteurs spécifiques.
- La recherche est actuellement dominée par les SCP à grande échelle tels que les réseaux intelligents et les services d'utilité publiques, dont beaucoup sont essentiels pour la sécurité nationale. L'innovation pourrait d'abord se produire d'abord dans ces secteurs.
- Un grand nombre de solutions d'avenir pourraient être développées dans des environnements non-militaires. Des partenariats de recherche pourraient être développés dans ces domaines d'application. Par conséquent, nous recommandons à RDDC de maintenir une vision globale lors de l'examen des orientations de recherche pour la cybersécurité des systèmes critiques.

Le tableau 2 résume les résultats du projet, conformément aux questions clés énoncée dans le mandat.

Tableau 2. Principales conclusions

Question	Conclusions
Systèmes de sécurité cyber-physiques (SCP)	• **Sécurité des réseaux**: les méthodes conventionnelles de sécurité, telles que l'authentification et la détection d'intrusion, ont dominé la recherche jusqu'à récemment. • **L'attention des chercheurs se déplace**: au cours des cinq dernières années, les solutions de sécurité ont dépassé la sécurité réseau conventionnelle pour se tourner vers des approches plus complexes, intégrées et multicouches (cyber-physiques). • **La sécurité, la fiabilité et la gestion des risques**: en raison de la nature essentielle de la plupart des systèmes cyber-physiques et à leur rôle dans la sécurité nationale, la sécurité, la fiabilité et la gestion des risques sont des éléments clés pour les stratégies de sécurité. • **Modélisation et simulation (M&S)**: un nombre croissant d'applications et de méthodes plus variées de M & S sont couvertes dans la littérature. • **Secteurs:** principalement les réseaux de capteurs sans fil, les réseaux intelligents (smart grid) et les services d'utilité publiques
Thèmes émergents SCP	• Modélisation et simulation • Cadres hiérarchiques • Intelligence artificielle, systèmes en mode agent, technologies prédictives • Modes d'attaques et technologies spécifiques (par exemple les attaques par injection des données, l'estimation d'état • Gestion des risques • Applications en temps reel
Grands joueurs SCP	• Les universités américaines sont dominantes, mais des recherches considérables sont en cours en Chine. Les entreprises commerciales sont également actives, souvent en collaboration avec des universités ou des laboratoires gouvernementaux • **Universités**: University of Illinois, Carnegie Mellon, University of California at Berkeley, Massachusetts Institute of Technology • **Entreprises:** Électricité de France, CESI Ricerca (Milan), MITRE Corporation, SRI International • **Organismes de recherche et de technologie**: Electronics & Telecommunications Research Institute (Korée du Sud), Royal Institute of Technology (Suède) • **Gouvernements**: Idaho and Sandia National Laboratories, National Institute of Standards and Technology (É.-U.) • **Organisations militaires**: Air Force Institute of Technology, Air Force Research Labs (NY/OH), National University of Defence Technology (Chine)Institute of Standards and Technology

Question	Conclusions
Sujets de modélisation/simulation	• Modèles et méthodes s'appliquant spécifiquement aux SCP, notamment les modèles menace/défense, les méthodes stochastiques, les modèles de Markov et les méthodes formelles • Environnements de modélisation hybrides, hiérarchiques, et dynamiques • Apport de la M&S pour la sécurité et la gestion des risques, par exemple, des logiciels / systèmes de bancs d'essai utilisés pour l'évaluation des risques
Thèmes émergents M&S	• Résilience, fiabilité, sécurité, risques • Systèmes en temps réel • Modes d'attaques et technologies spécifiques, par exemple les attaques par injection des et l'estimation d'état • Intelligence artificielle, les systèmes en mode agents, les technologies prédictives • Réseaux intelligents et autres applications, comme par exemple l'industrie automobile
Joueurs M&S	• Un plus grand niveau de participation internationale est observé pour les sujets M&S que pour la sécurité des SCP en général • Les joueurs sont généralement les mêmes pour la M&S et la cybersécurité générale (voir ci-dessus), à l'exceptions de quelques organisations qui sont surtout actives en M&S, soit Texas A&M University, Missouri University of Science & Technology, Northwestern Polytechnic (Chine), et l'Insitut Fraunhofer (Allemagne)

This page intentionally left blank.

NRC-CISTI
Canada Institute for Scientific and Technical Information
INFORMATION > INSIGHT > INNOVATION

STI Assessment

Title	**Cybersecurity of Critical Systems : Literature Survey**
Project Numbers	STI 14926, DRDC SRE 07-001-033
Date	February 2013
Prepared for	Dr. François Bernier, DRDC Valcartier Mission Critical Cyber Security Support 6-5-2(C) - C41SR,
Prepared by	Brenda Brady
Contact	Brenda.brady@nrc-cnrc.gc.ca, (902) 367-7552

National Research Council Canada
Conseil national de recherches Canada
Canada

DRDC Valcartier CR 2013-188

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

1 BACKGROUND

1.1 Context

DRDC's section on Mission Critical Cybersecurity is drafting proposals for research activity to be conducted for its Canadian Forces clients. In order to plot research directions and build on existing knowledge, they have commissioned this overview of the state of the art of security for cyber-physical and embedded systems.

The rapid growth of networked systems and their integration with critical (physical) infrastructures and systems has exposed these systems to new threats. Cybersecurity in this environment is especially challenging since these systems combine both "cyber" and physical components such as hardware, software, networks and physical elements. Attacks may target an individual component or multiple vectors, each of which may be dependent or linked to others. The combined or cascading effect may be catastrophic.

The current project builds on a previous STI/DRDC study on resilient complex systems.[1] In that instance, resilience was engineered in response to a variety of threats, not all of them related to cybersecurity. Of particular interest for the present study are resilient, survivable systems for cyber-physical and embedded systems, and especially components of resilience that are more specific to these types of systems and not simply based on the classical methods of network/host-based security and intrusion detection (such as authentication, certification, or event logging). In a cyber-physical environment, resilience may be based on dynamic and deterministic physical control frameworks (for example, voltage regulators) or techniques such as the use of consensus algorithms or decision making agents to control systems. A real-time operational environment presents additional challenges, since threat detection and response must occur quickly.

The current project will also focus on how modeling and simulation (M&S) and similar techniques can be used as part of an improved cybersecurity strategy for resilient cyber-physical and embedded systems in critical missions.

The critical systems and infrastructures under consideration include key military applications such as computer network-controlled autonomous vehicles, vehicle platforms, weapons systems, air traffic and navigation control, satellites and command and control, but also applications in civil defence or industries where networks control critical mission elements and/or where infrastructures could be threatened by malicious attacks. Sectors include aviation, smart grids, automotive sensor and navigation nets, industrial processes, medical devices, machine to machine networks, gas pipelines, water treatment and supply. Embedded systems in portable devices or supervisory control and data acquisition systems may also be implicated, for even an attack on a single sensor or device may compromise security for a system or an entire network.

1.2 Key Issues

The results of this study are intended to provide DRDC researchers with a solid perspective as they build a research portfolio in the area of cybersecurity for critical and/or embedded systems. The first step in designing this research will be to understand what is currently being researched and published in the domain, with particular emphasis on cyber-physical systems (CPS) or embedded systems for the military, homeland security, public security, or industrial control applications. The study results will also assist the team as it explores the role of modeling and simulation in cyberdefence of critical systems.

1.3 Key Questions

1. Which defensive or preventive methodologies (platforms, tools, techniques, models, simulations, engineering or design methods) are currently being researched in relation to cybersecurity for cyber-physical and/or embedded systems? Which infrastructures or systems are addressed, and which sectors or industries are most active?
2. What are the emerging research trends for these technologies?
3. Who are the major players (government, military, academic and commercial) in the domain of CPS/embedded systems + cybersecurity/resilience? Who are the main authors?
4. As a subset of question 1, which modeling and simulation approaches are currently being researched in relation to cybersecure, cyber-physical or embedded systems? How do these approaches address resilience?
5. What are the emerging research trends for these approaches or technologies?
6. Who are the major players (government, military, academic and commercial) in the domain of M&S for secure, resilient cyber-physical or embedded systems? Who are the main authors?

2 INTRODUCTION

To address the mandate questions, a comprehensive literature search was conducted in various scientific and technical databases and web resources. A complete description of the search strategy is found in Section 9.2 of this report.

After deduplication and weeding, a total of 2,220 bibliographic records for journal articles, conference proceedings, theses, technical reports and other scientific or technical documents published between 2003 and 2013 were retained and loaded into the VantagePoint and Intellixir platforms for processing and analysis.[a] This dataset is referred to as the Master dataset in the analyses which follow. A sub-database of 1,004 records, isolating all records which referenced modeling and simulation (M&S) was used to address questions 4-6 of the mandate.

[a] VantagePoint is a desktop client produced by the US firm Search Technology; Intellixir is a web-based platform installed on a secure NRC server and produced by the French company Intellixir. The two datasets used for this report have also been made available to DRDC for a limited period of time on the Intellixir server.

3 CYBER-SECURITY FOR CRITICAL SYSTEMS

3.1 Major Research Topics

A review of recent syntheses and review articles showed that common areas of research in this domain are wireless sensor networks and critical infrastructure such as electrical power grids. Wireless sensor networks are a key component of both military and industrial control/communication networks, and the electrical grid enables critical activity at many levels. Cyber-physical systems (CPS) such as these are especially vulnerable, however, and present many challenges for security. For instance:

- CPS are subject to many different types of attack – almost as many as there are types of cyber-physical system – and these are becoming more varied and longer-lasting.[2-10]
- CPS systems are often unattended, remote, and distributed; their isolation and distribution leaves them exposed to threats on many fronts. Many were never intended to be connected to the Internet, which also increases their vulnerability.
- Many CPS are resource-constrained: restrictions to power and memory cannot handle the processing associated with security policies and defence mechanisms.
- CPS combine many components and systems that interact with each other in a complex fashion, often in many hierarchical layers; security solutions should also be deployed in layers.
- CPS often comprise a large proportion of older (legacy) components or technologies, making detection and defence difficult.
- Many CPS are under the control of private enterprise; private-public partnerships may be required to fully address cybersecurity challenges.
- CPS are often mission-critical and operate in real-time: safety, resilience/survival, synchronicity and speed of response should be part of the security strategy.

In response to these many types of challenges, researchers have observed that traditional cybersecurity frameworks, such as firewalls, authentication, network intrusion detection, or techniques that target denial of service attacks, are not enough. For example, Karen Goertzel of Booz Allen Hamilton wrote in 2009:

> Organizations dependent on mission-critical systems and networks are recognizing that the traditional "protect-detect-react" (PDR) strategy for countering intrusions and attacks is ineffective. A new information assurance and cybersecurity strategy is needed that augments PDR with the ability of systems and networks to "fight through" attacks.[11]

An evaluation of traditional security solutions as they apply to supervisory control and data acquisition (SCADA) systems also noted the importance of safety, reliability, and continued system availability:

> Unfortunately, the operating parameters and security principles associated with traditional IT systems do not readily translate to the SCADA environment. Security solutions for IT systems focus primarily on protecting the confidentiality of system and user data. Alternatively, SCADA systems must adhere to strict safety and reliability requirements and rely extensively on system availability.[12]

According to the recent literature, better CPS models are required: models that are context-aware, industry or application-specific, stochastic (behavioural), intelligent (learning), cross-layer and state estimation-based, and recognizant of both temporal and spatial elements. CPS attack models should also consider survivability. Such models can be used as part of systems engineering/design, but can also be used to develop risk assessments and

threat/defence evaluations for existing systems. However, according to some recent analyses, such secure, resilient and trustworthy systems are "in their infancy".[13-17]

These reviews can serve as a useful point of departure. The themes they introduce suggest avenues of inquiry which, along with the project's key questions, can be explored in this analysis as well as in future research.

3.1.1 Master Dataset: Topic Correlations

To obtain a birds-eye view of the data, to understand how sub-topics differ by volume, and to discover how issues, methods, infrastructures and applications correlate, the top 300 terms (keywords) in the master database were plotted in cluster maps using TouchGraph Navigator software. Since the maps do not fit on a printed page, the complete cluster maps are provided in Appendix 1 (Figure A), attached to this report. Excerpts from these maps are shown below.

TouchGraph's clustering algorithm clusters terms together based on statistical similarity to each other (i.e. word co-occurrences) and dissimilarity with other clusters. Generally, a cluster illustrates a self-contained group of concepts that is independent from (though still connected to) the rest of the graph.

The size of the nodes in the main maps and excerpts represents the relative number of publications associated with each node, and the lines in between nodes show the correlation coefficient (multiplied by 100) between two nodes. Only correlations of 20% or greater are shown. Certain redundant nodes have also been suppressed here, and additional views of nodes with no correlation at this level of filtration are included in Appendix 1, Figure B.

Several notable trends emerge from the map shown in Appendix 1, Figure A. A dominant red cluster with large bubbles shows a large proportion of database content for topics such as wireless sensor networks (WSNs) and network-centric cybersecurity methodologies such as authentication, cryptography, network protocols, and intrusion detection. Cybercrimes such as denial of service or wormhole attacks and jamming show a strong relation to WSNs. Over the decade covered by our inquiries, this type of cybersecurity discussion has clearly been dominant.

In an excerpt from the main map, critical infrastructures and system types such as the power grid (turquoise and green clusters, Figure 1) are shown linked to cybersecurity, resilience, supervisory control and data acquisition systems (SCADA) , and industrial controls. In Figure 2, the yellow cluster connects embedded systems to cybersecurity and CPS as well as areas of apparent particular vulnerability or importance, such as resilience, real time, physical domain, and operating systems (OS). The articles which correspond to these linkages discuss various aspects of software/OS vulnerability and how real-time environments and physical considerations add complexity to security solutions).[18-20] The generic term *Modeling* is also shown linked to cyber-physical security systems (upper right, Figure 2).

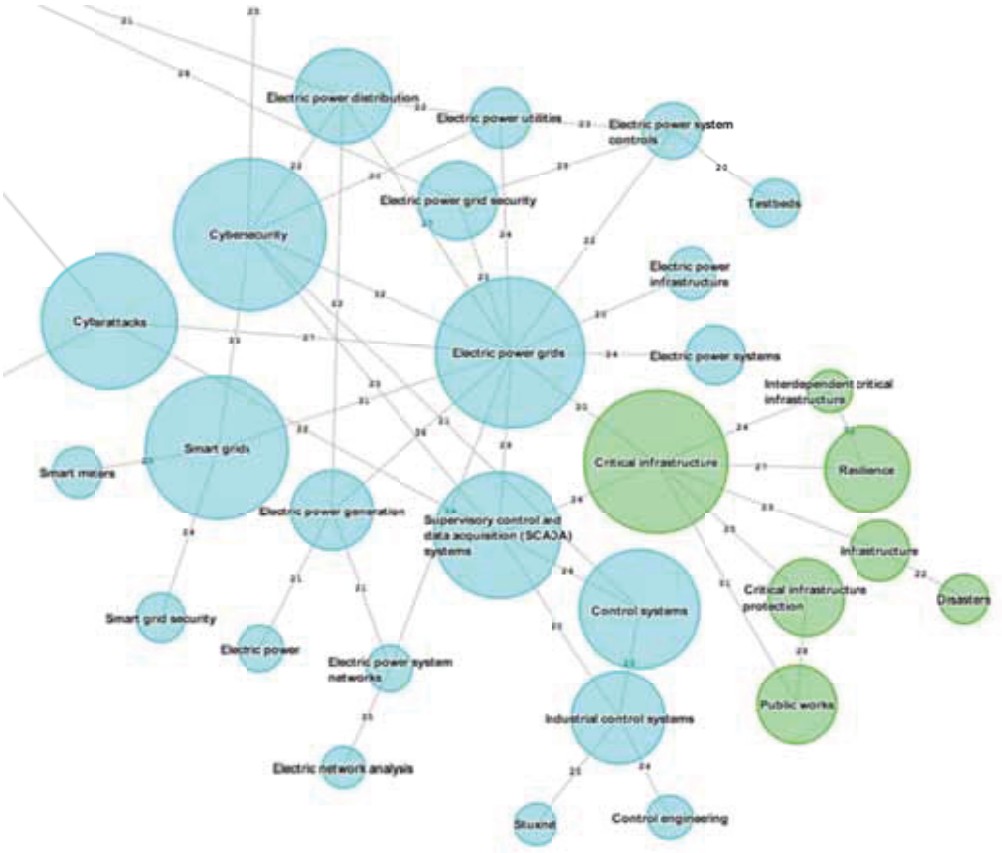


Figure 1. Master Dataset: Excerpt from Cluster Map of Top 300 Terms, Correlation ≥20%: Smart Grid, SCADA Systems, Controls and Resilience

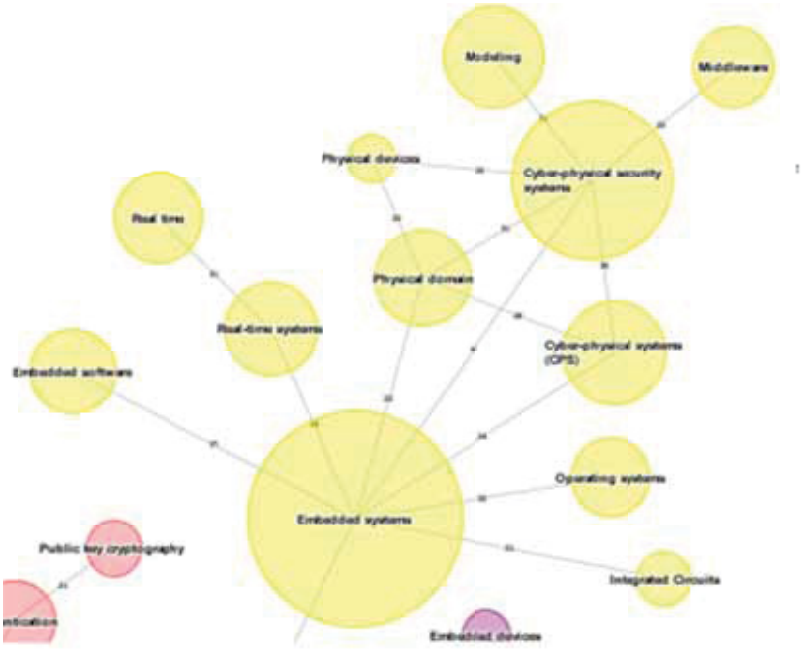


Figure 2. Master Dataset: Excerpt from Cluster Map of Top 300 Terms, Correlation ≥20%: Embedded Systems, Real-Time, Physical Domain, Operating Systems, Modeling

A beige cluster excerpted from the Master dataset map of terms also demonstrates the importance of topics such as safety, risk or reliability assessment, and fault tolerance.

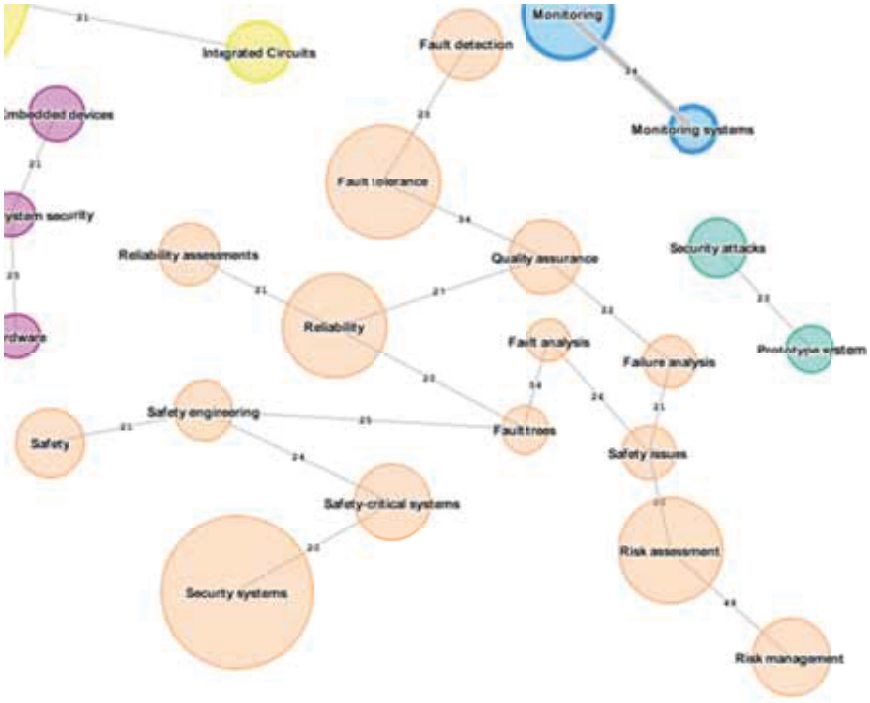


Figure 3. Master Dataset: Excerpt from Cluster Map of Top 300 Terms, Correlation ≥20%: Reliability and Risk Cluster

By suppressing some of the network and telecommunications nodes in the main map and by lowering the correlation filter to ≥15, one obtains a slightly more detailed view which is less network-centric. A complete view of this map is provided in Appendix 1, Figure C, and comments on it are provided below.

In this alternative map, one can see a greater incidence (albeit at lower percentages) of correlation within the WSN (red), embedded systems (yellow), and the electrical grid (turquoise) clusters. Compared to the original map (Appendix 1, Figure A), additional application areas appear here: *Nuclear power plants, Water distribution systems, Medical devices, Military communications*, as well as some specific methodologies (*Trust management, Agent-based systems, State estimation* to protect against *False data injection attacks, Formal methods, Markov processes*). In excerpts from the alternative-view map modeling and simulation terms are also shown linked to *Hardware-software* and *Testbeds* (Figure 4) and to *Software reliability* (Figure 5). Concepts of recovery and resilience are also more apparent throughout the entire view.

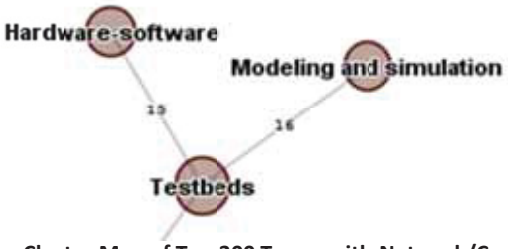


Figure 4. Master Dataset: Excerpt from Cluster Map of Top 300 Terms with Network/Communications Nodes Suppressed, Correlation ≥15%: Hardware-Software/Modeling/Testbeds

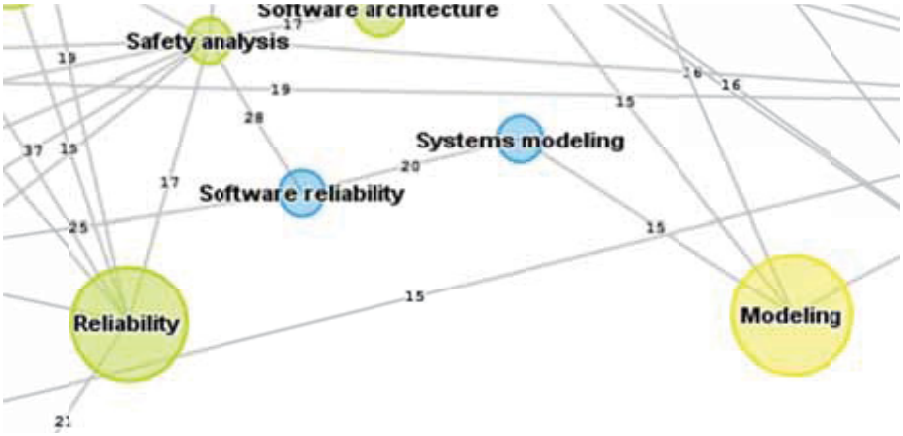


Figure 5. Master Dataset: Excerpt from Cluster Map of Top 300 Terms with Network/Communications Nodes Suppressed, Correlation ≥15%: Linked Nodes for Reliability and Modeling

3.1.2 Subject Groups

In another approach to identifying major topics, subject groups were created from terms in the keyword field. The groups reflect subjects with high publication counts, questions in the mandate, and trends suggested in the review literature. Figure 6 shows a list of the top 21 subject groups ranked by the number of publications associated with each group.

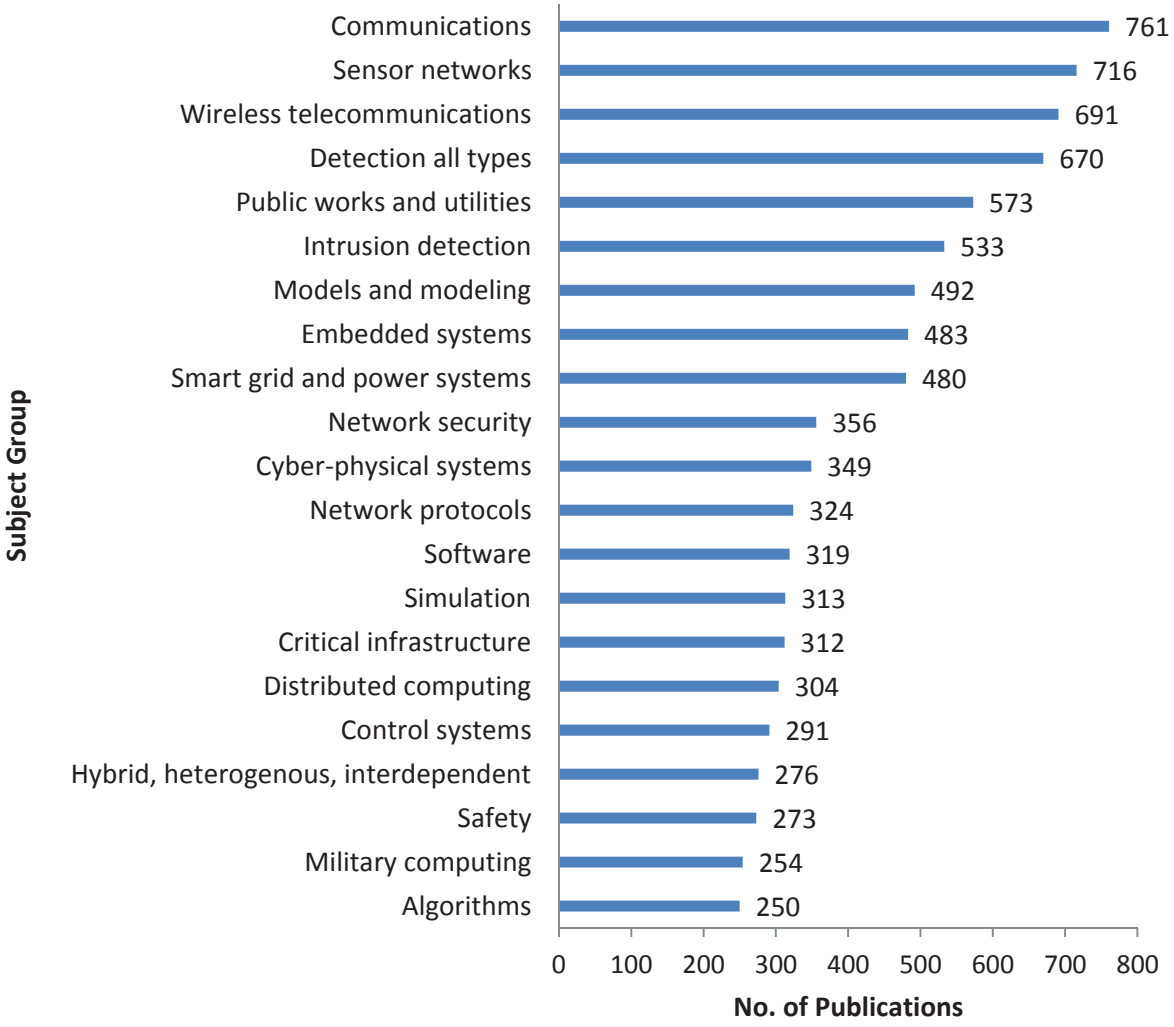


Figure 6. Master Dataset: Top Subject Groups, ≥250 Publications

Figure 6 confirms many of the same emphases found in the topical cluster maps: the same dominance of sensor networks, telecommunications, public utilities, and network-related aspects of cybersecurity. In this listing, the group label *Hybrid, heterogeneous, interdependent* tries to capture the many instances in the dataset of security solutions using these adjectives. In these articles, CPS are generally described as complex systems that combine many differing sub-elements or layers, are interactive, and while physical in nature, depend on information technology for their management and control.

Subject groups were also categorized according to genre, using three major streams suggested by the key questions:

1) methods or techniques of modeling or data processing
2) features or attributes (of either cyber-physical systems or their security solutions)
3) sectors or application areas

Figures 7-9 show subject group rankings by these genres. In Figure 7, the label *Hierarchical frameworks* refers to layered security architectures, some of which may use *Middleware* services to handle security-related communications between layers. *Behavioral/stochastic analysis* describes solutions in which typical and atypical, predictable and wildcard system behaviours are modeled in order to provide probabilistic (stochastic) analyses.

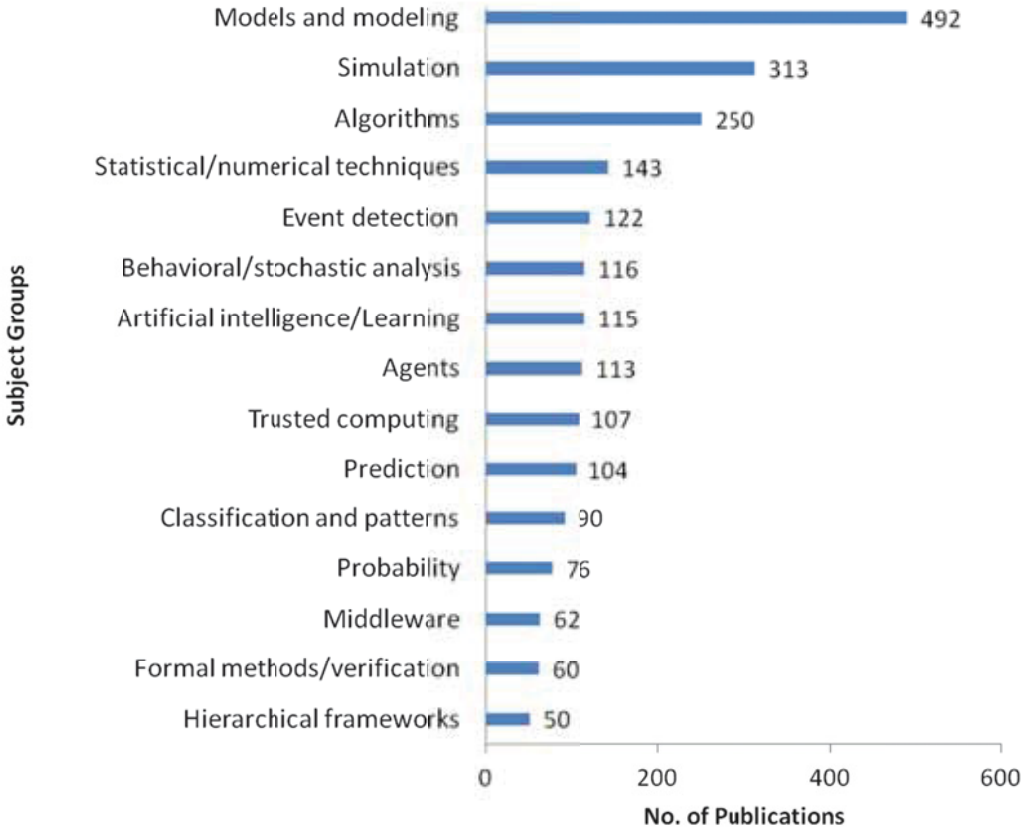


Figure 7. Master Dataset: Top Subject Groups: Methods or Techniques

Figure 7 confirms the importance of modeling and simulation as a technique in support of cybersecurity for CPS. The sub-types captured in this list appear to describe a combination of traditional (e.g., *Classification and patterns, Trusted computing*) and more advanced techniques (e.g., *Behavioral/stochastic analysis, Artificial intelligence/Learning, Agents, Middleware, Prediction*).

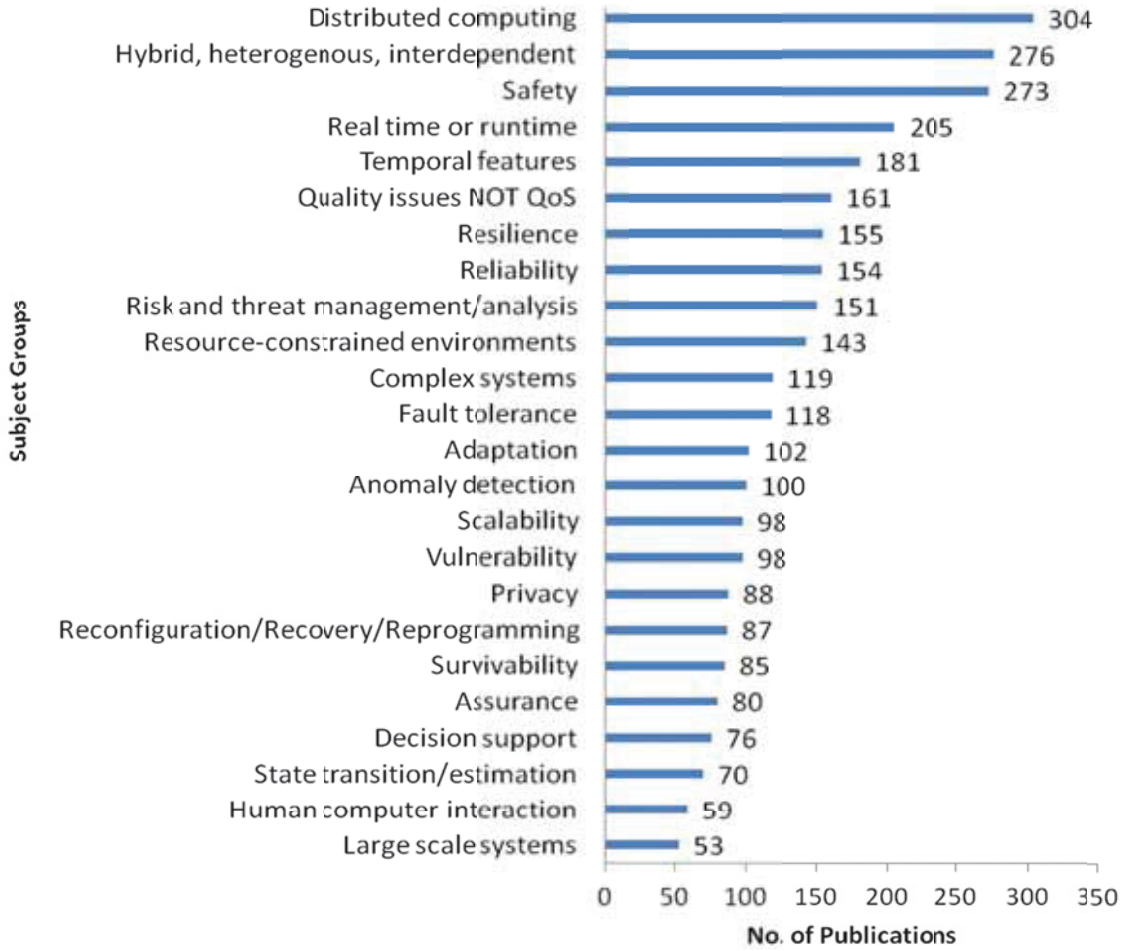


Figure 8. Master Dataset: Top Subject Groups: Features or Attributes

Figure 8 describes features or attributes of cyber-physical systems and the security solutions that protect them. This graphic attests to the complexities of the CPS environment (*Distributed, Hybrid, Large scale, Resource-constrained*, etc.) and also shows the emphasis in the literature on both safety and resilience.

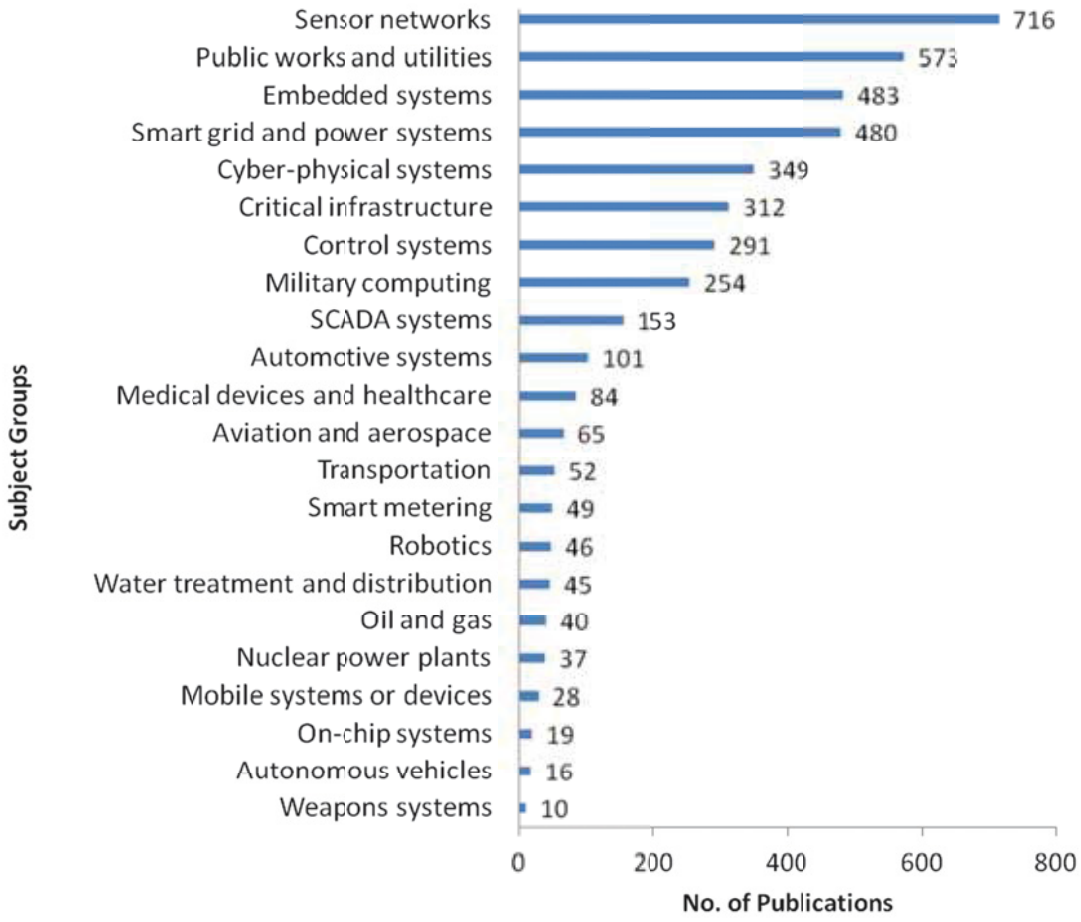


Figure 9. Master Dataset: Top Subject Groups: Sectors or Application Areas

In Figure 9, a listing of sectors or application areas, one sees the dominance of certain types of cyber-physical environments in the security literature. Sensor networks (of all types) top the list, and there is also frequent mention of generic systems (*Embedded, Cyber-physical*, etc.). Public works and utilities, especially the smart grid, are of concern, but automotive systems and control systems (the latter usually industrial in nature) also appear.

3.2 Emerging Research Trends

To detect changes over time and to identify topics which appear to be gaining research interest, we began by plotting the numbers of publications from 2003 to 2012 (Figure 10). Data from 2013 were excluded from this view, since numbers for the current year are incomplete. This figure shows a steady increase in the number of publications from 2003 to 2011, and then a marked decrease in 2012.

Overall, the upward trajectory suggests strong and sustained interest in the field of cybersecurity for cyber-physical systems: for instance, there is no evidence of a sigmoid (S) curve that is typically seen in subjects approaching maturity. However, the decline at the end of the period is puzzling, and several possible influences that might explain the change were investigated. For instance, the absence of publications from an important conference not held for several years might explain the post-2011 dip, however conference publications are in strong evidence all through the decade, including the era post-2011. There is also no evidence of a decline in contributions from major geographic regions such as China or the United States, such as might be attributable to changes in research funding or government policy.

One possible explanation may lie in diminishing publications from certain subject groups, such as those related to sensor networks, communications and wireless telecommunications. These are all large volume groups, and they do decline somewhat at the latter end of the decade measured (Figure 11).

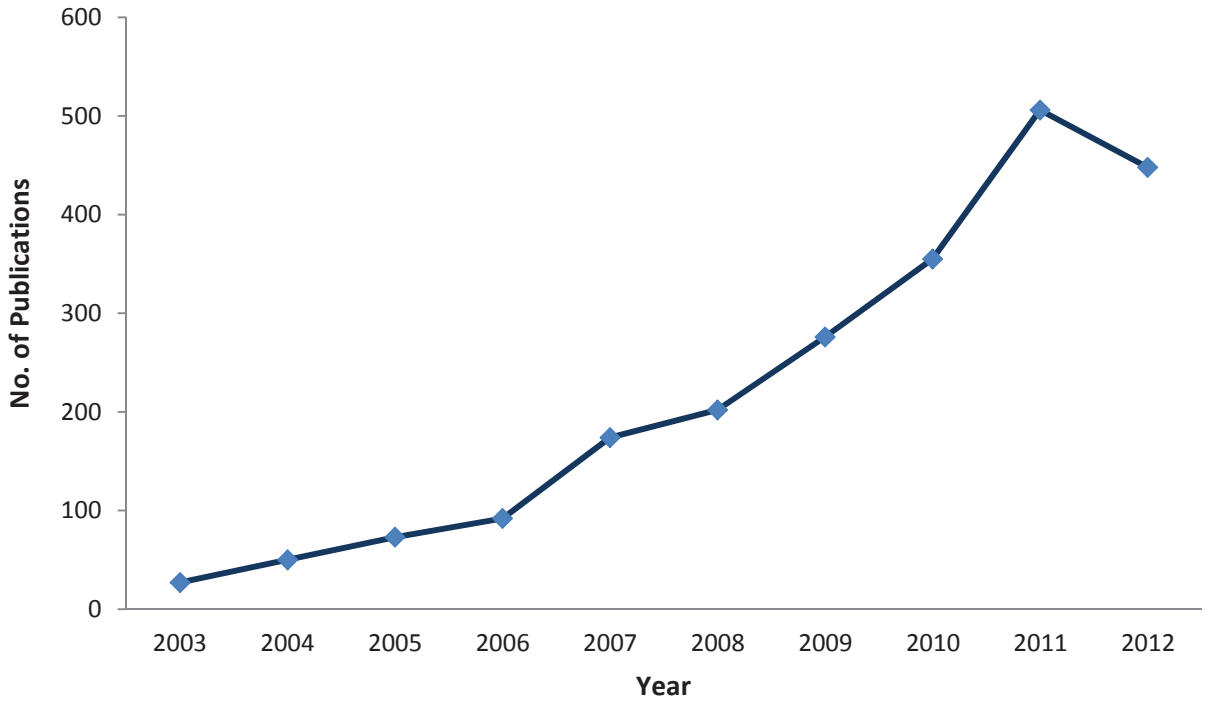


Figure 10. Master Dataset: Numbers of Publications, 2003-2012

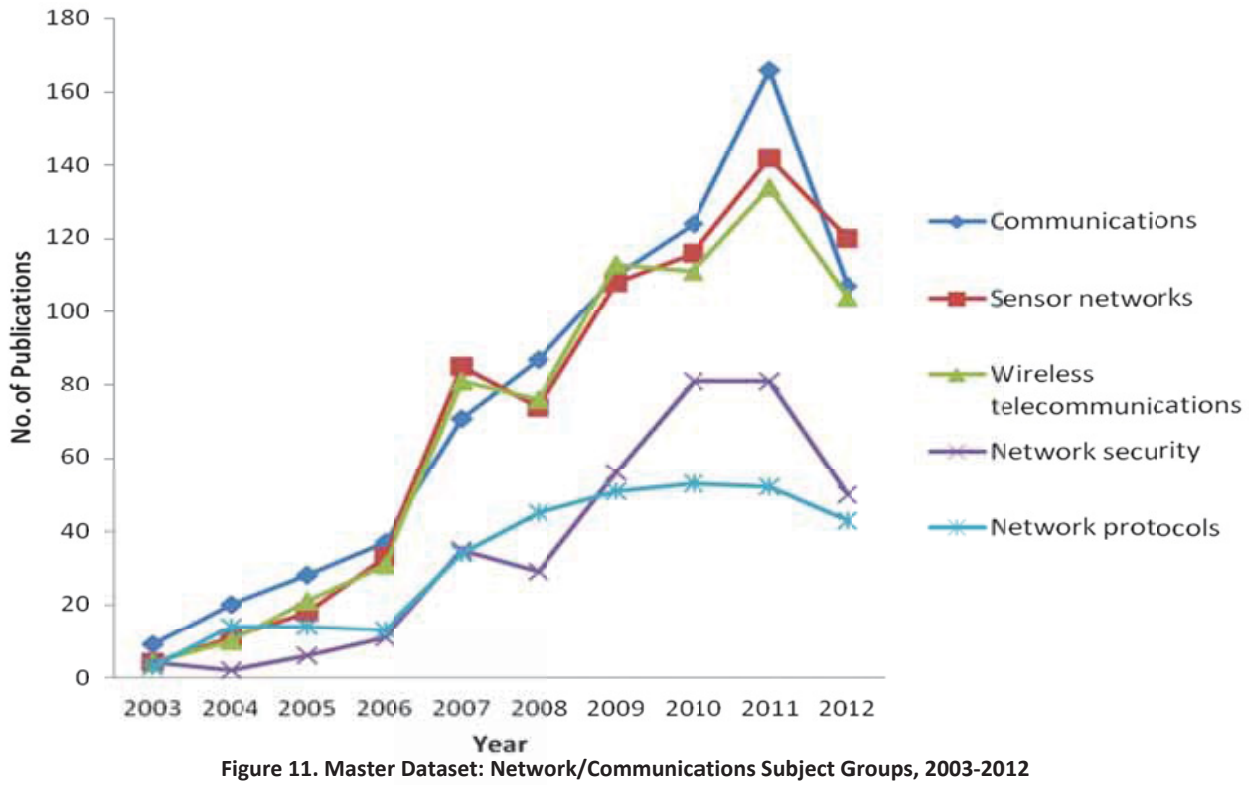


Figure 11. Master Dataset: Network/Communications Subject Groups, 2003-2012

Given the publication patterns seen in Figure 10 and 11, it becomes all the more interesting to review the performance of subject groups which demonstrate *stable or ascending* numbers of publications at the end of the period, and to calculate the normalized values for publication performance. Taken together, these analyses indicate topical areas deemed to be of highest interest or emergent in the field of CPS security.

In the analyses which follow, data are presented according to subject group genres: *Methods or Techniques, Features or Attributes*, and *Sectors or Application Areas*. For each of these categories, an initial graphic shows sub-topics with rising or stable publication numbers for the period 2010 to 2012. This is followed by a review of normalized rates of publication.

In all three views of rising publication trajectories (Figures 12, 14, 16), we see small numbers of articles -- usually five or less per annum -- at the beginning of the period. In the *Methods or Techniques* genre (Figure 12), the performance of some groups (*Models and modeling*, *Algorithms*, and *Behavioral/stochastic analysis*) shows a dramatic increase.

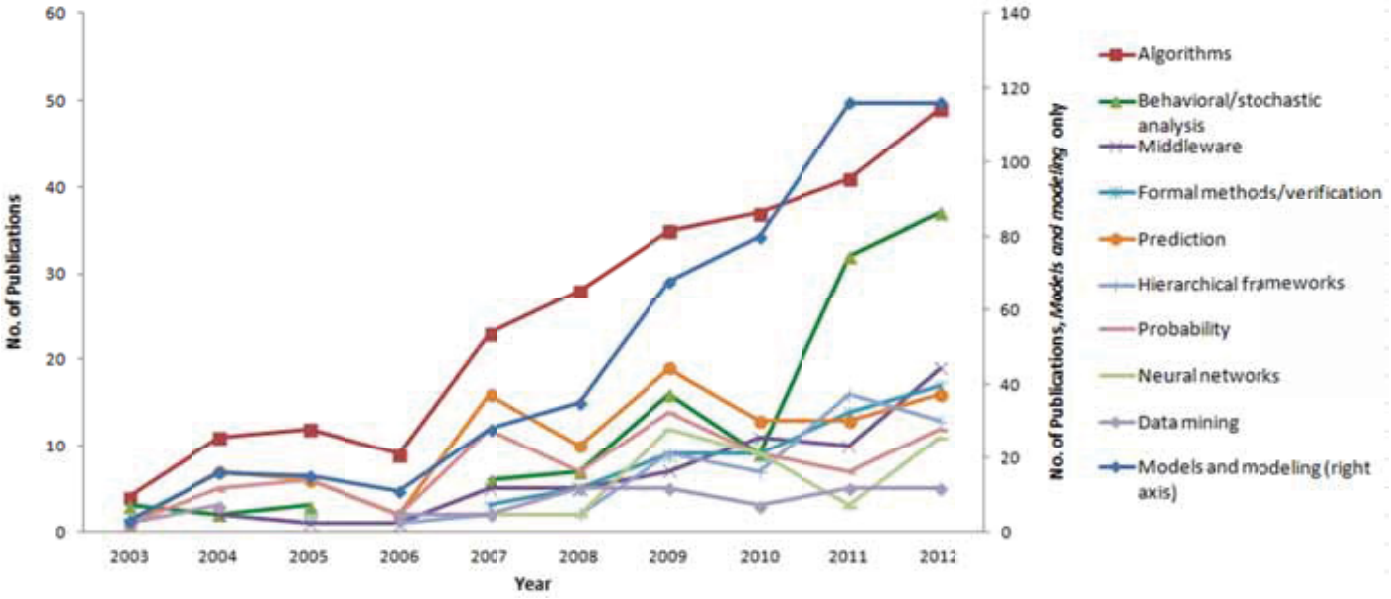


Figure 12.Master Dataset: Methods or Techniques with Rising Numbers of Publications, 2003-2012

In order to determine which topics in CPS/security research are showing the fastest relative growth rates over the past 10 years, an analysis was performed based on linear regression of the growth rate of numbers of records per year. A more detailed description of the methodology is provided in Section 9.2 of this report. Topics with positive values may be considered as those demonstrating a higher degree of research interest for the time period measured, relative to other topics in the group. Negative values do not mean that interest is declining, only that these topics have a slower growth rate relative to the others.

When the normalized rates of publication are computed for the *Methods or techniques* category, the large, generic subject group *Models and modeling* has the fastest growth rate, relative to other subjects in this category. *Behavioral/stochastic analysis* also demonstrates a positive value, however *Algorithms*, a high-volume group which is shown as increasing post-2006 in Figure 12, plots slightly on the negative side of the standard deviation. Topics with both rising publication numbers (Figure 12) as well as an overall high rate of interest (Figure 13) are *Hierarchical frameworks* and *Prediction.* Figure 13 speaks to the importance of artificial intelligence, agent-based computing, and methods such as game theory in handling complex and dynamic security threats.

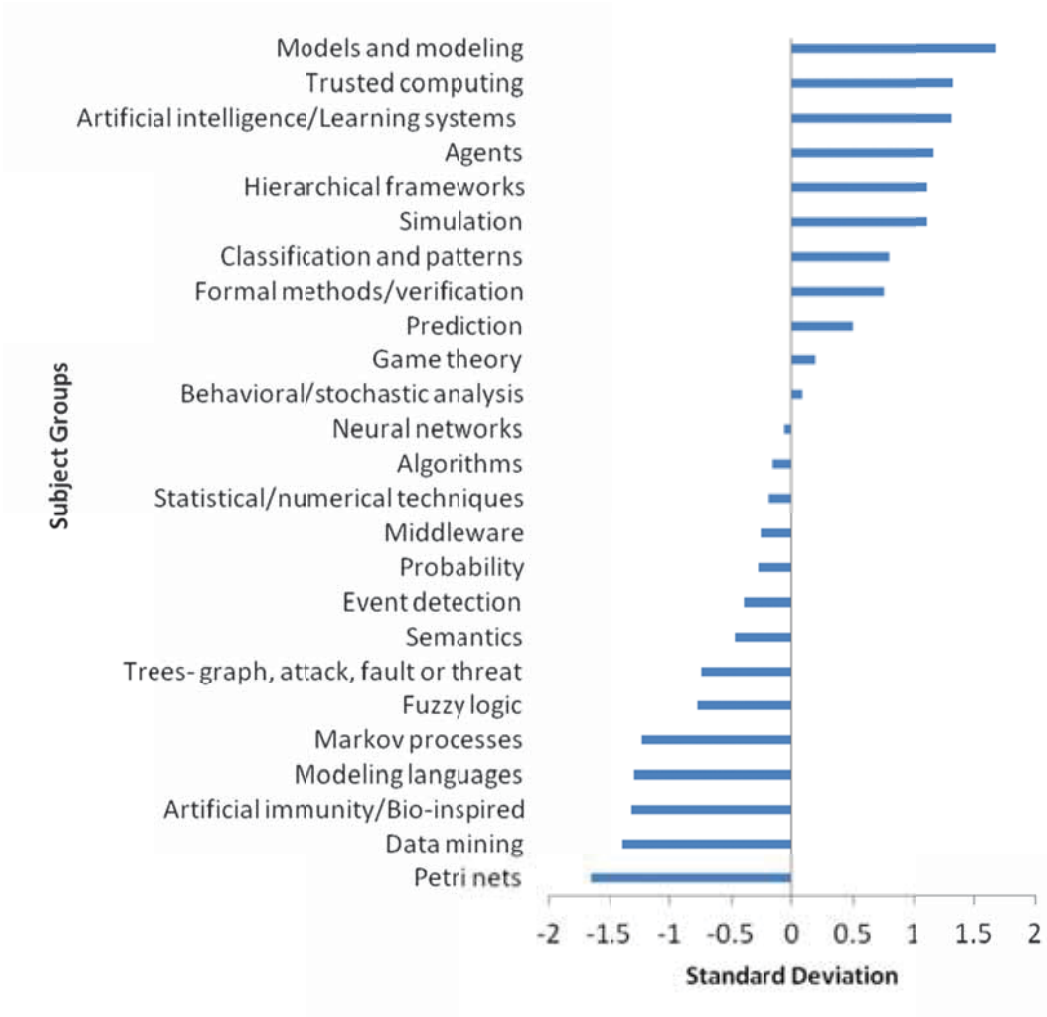


Figure 13. Master Dataset: Methods or Techniques: Relative Rate of Research Interest, 2003-2012

Of the thirty-three sub-topics grouped in the category *Features or Attributes*, only eight display a rising trajectory of publication at the end of the decade measured. Publication patterns for these topics demonstrate some erratic peaks and valleys, but a gradual rise overall. In this view (Figure 14), *Resilience* and *Data injection attacks* show particularly strong upward movement.

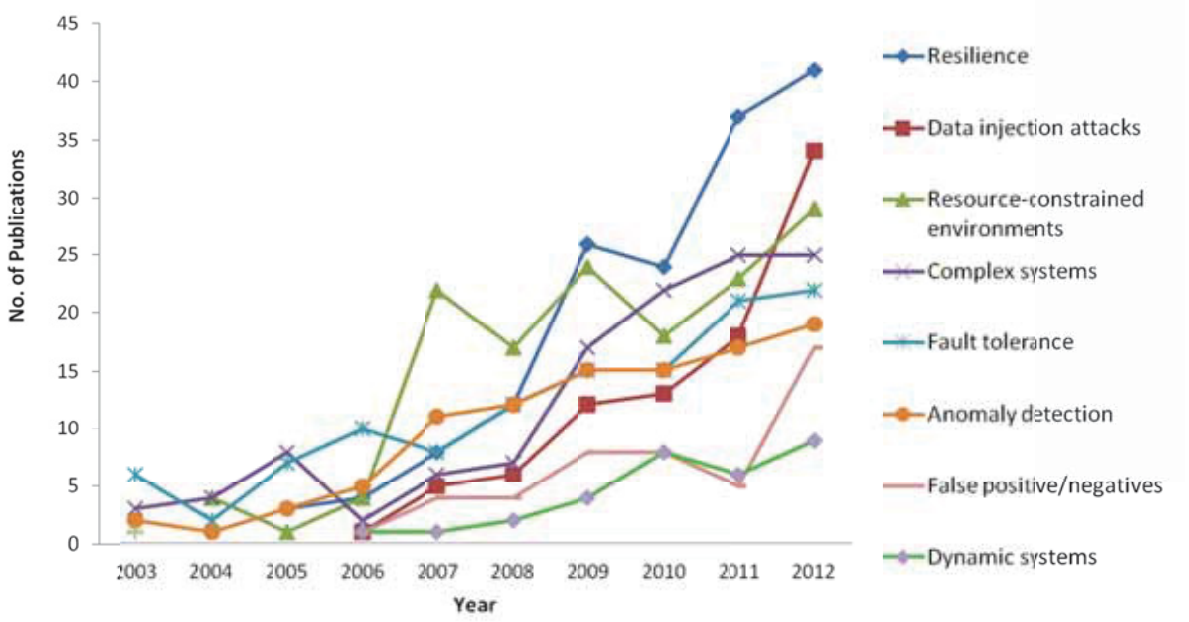


Figure 14. Master Dataset: Features or Attributes with Rising Numbers of Publications, 2003-2012

Several of these features or attributes also have strong rates of research interest (Figure 15): *Resilience, Data injection attacks, Anomaly detection, False positives/negatives*, and *Dynamic systems* all show both rising publication numbers *and* strong research attention overall. In addition, the normalized list speaks to rising interest in areas such as *Risk analysis, Reliability, Real time* and *Reconfiguration or recovery*, as well as the *Hybrid, heterogenous and interdependent* nature of systems in CPS environments. *Distributed computing* also ranks high in Figure 15, possibly because of the extra degree of vulnerability it confers, and the temporal and well as spatial dimensions it adds.

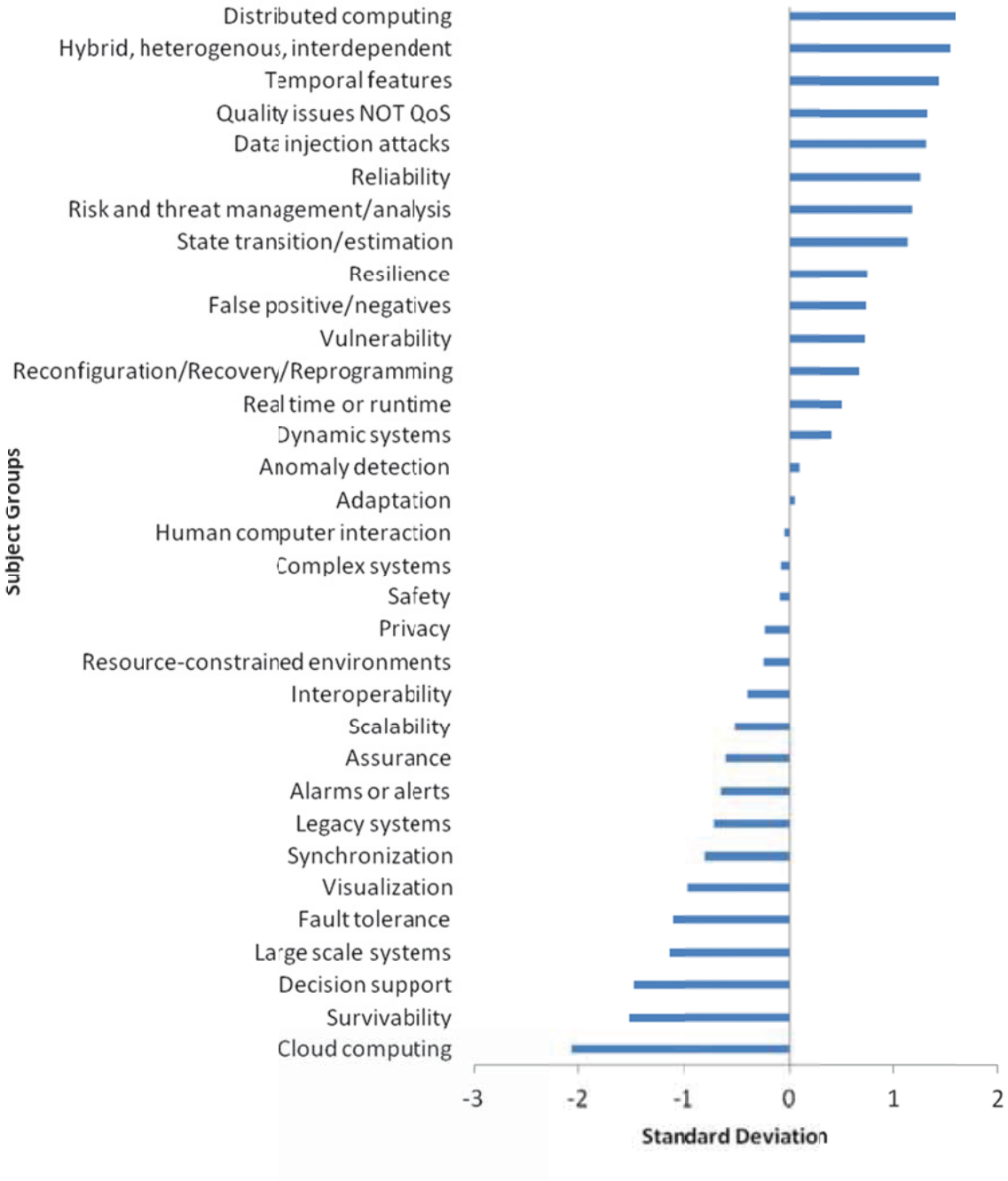


Figure 15. Master Dataset: Feature or Attributes: Relative Rate of Research Interest, 2003-2012

In Figure 16 (*Sectors or Application Areas*) the generic label *Cyber-physical systems* grows exponentially, while more specific topics such as *Control systems, Physical domain*, and *Automotive systems* also show especially strong upward trajectories.

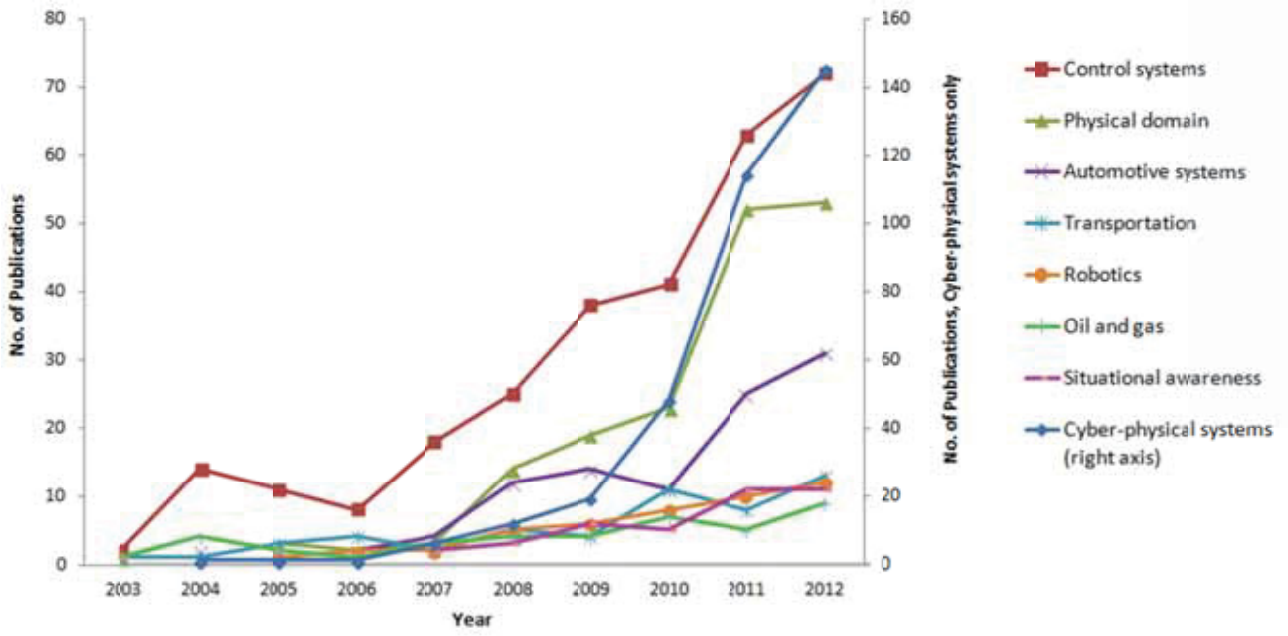


Figure 16. Master Dataset: Sectors or Application Areas with Rising Numbers of Publications, 2003-2012

Figure 17 indicates that most of the subject groups with rising numbers post 2008 – *Cyber-physical systems, Physical domain, Automotive systems, Transportation, Robotics,* and *Situational awareness* have demonstrated sustained or growing rates of research interest . Topics such as *Smart grid, Smart metering, Public works and utilities*, and *Critical infrastructure* also appear with positive values in Figure 17, suggesting that industrial applications and infrastructures such as the electrical grid, which are associated with national security and economic activity, are high on the research agenda. *Sensor networks* also rank high in terms of growing interest; this is not surprising since sensors are part of most CPS applications.

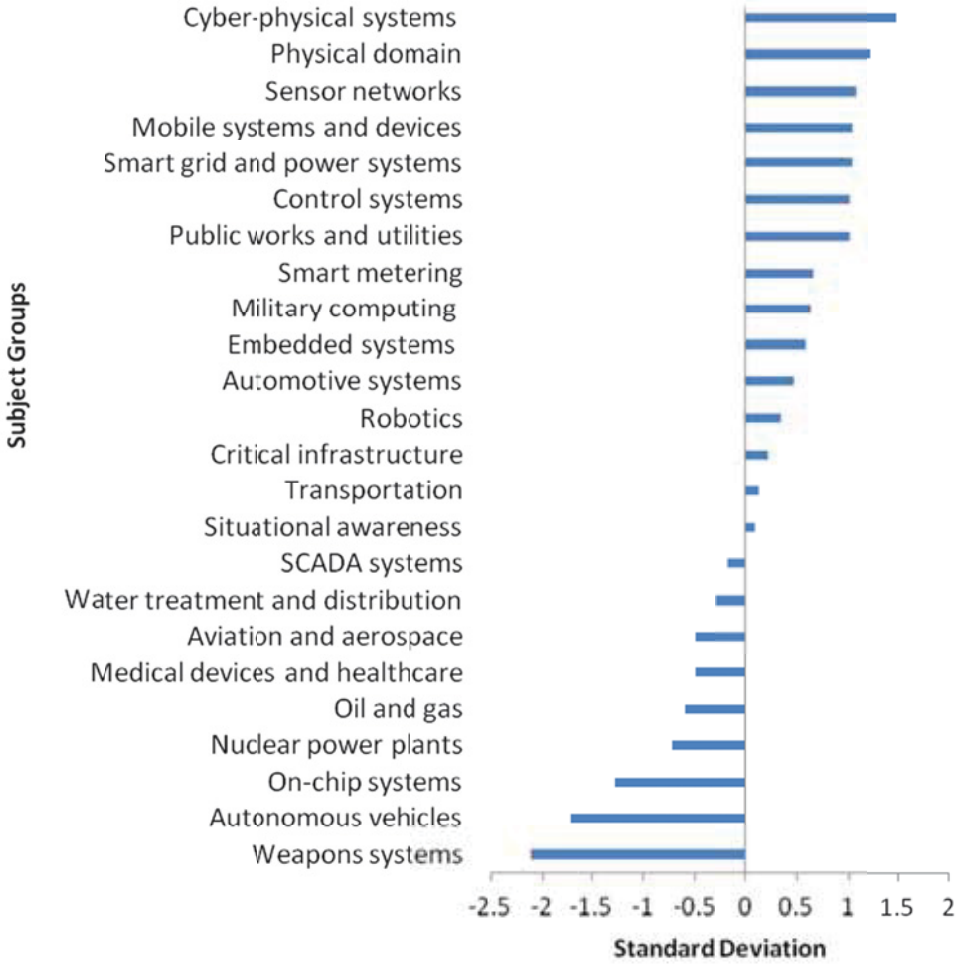


Figure 17. Master Dataset: Sector or Application Areas: Relative Rate of Research Interest, 2003-2012

3.2.1 Summary of Emergent Topics

Analysis of the records in the Master set documents key research topics according to several different indicators, including overall tallies by subject groups, changing publication patterns, and normalized rates of publication.

Counts by volume demonstrate that wireless sensor and communications networks and fairly conventional methods of cybersecurity, such as cryptography and firewalls, are still very much on the research agenda. As the attention of researchers turns to cyber-physical, embedded, or SCADA systems, however, and as more sophisticated attacks occur, the increased complexity of the security issue becomes apparent. As the focus of research shifts gradually to include a broader set of problems and behaviours – as research considers the special parameters and conditions found in systems such as the electrical grid -- different approaches are seen. These second-generation approaches can be detected by examining topical clusters with a high degree of correlation, subject groups with rising publication trajectories (especially in the last few years), and topics with rising normalized rates of publication. Artificial intelligence, hierarchical frameworks, agent-based and predictive methods are typical of these second-generation approaches.

Our analyses suggest that modeling and simulation are a critical part of security solutions for the cyber-physical world. Modeling and simulation techniques apply to both the cyber (software, networks) and physical (hardware, devices, sensors) elements. Thorny issue areas emerging in the literature are the hybrid, components-based, real-time nature of CPS networks, which also tend to be large and widely distributed, adding to vulnerability and complexity.

In the CPS environment, concepts such as resilience and reliability resonate and are also attracting increasing research attention. These topics are also linked to safety, regulation and insurance; entire power grids or other critical infrastructure, key to national and economic security, may be at stake. Predictive and evolutionary techniques based on artificial intelligence, agents, state-estimation, and game theoretic models are well suited to this complex and dynamic environment and also figure prominently on the list of topics showing growing research interest. Formal methods can be used as part of strategies to develop and verify systems.

Based on volume counts and topical correlations, it appears that much of this CPS research is being driven by large systems such as wireless sensor networks, the electronic grid or other public utilities. However, as seen in Figures 16 and 17, automotive systems, mobile devices, transportation, robotic and military applications are also the focus of increasing attention.

3.3 Major Players

3.3.1 Geographic Distribution

An analysis of geographic distribution of the author affiliations associated with articles in the master dataset shows research strength in the following top jurisdictions:

- United States (881 articles, or 39.7% of the dataset)
- China (335 articles or 15.1%)
- South Korea (94 articles, or 4.23%)
- Germany (88 articles, or 3.9%)

Canada contributes only 74 articles or 3.3% of the dataset. The publication counts for all countries also include instances of international co-publication. Such collaborations appear to be rather slight for this database: in over 2,200 articles, there are 23 co-publications between the U.S. and China; only U.S.-French collaboration, at 31 articles, exceeds the rate of Sino-American co-publication.[b]

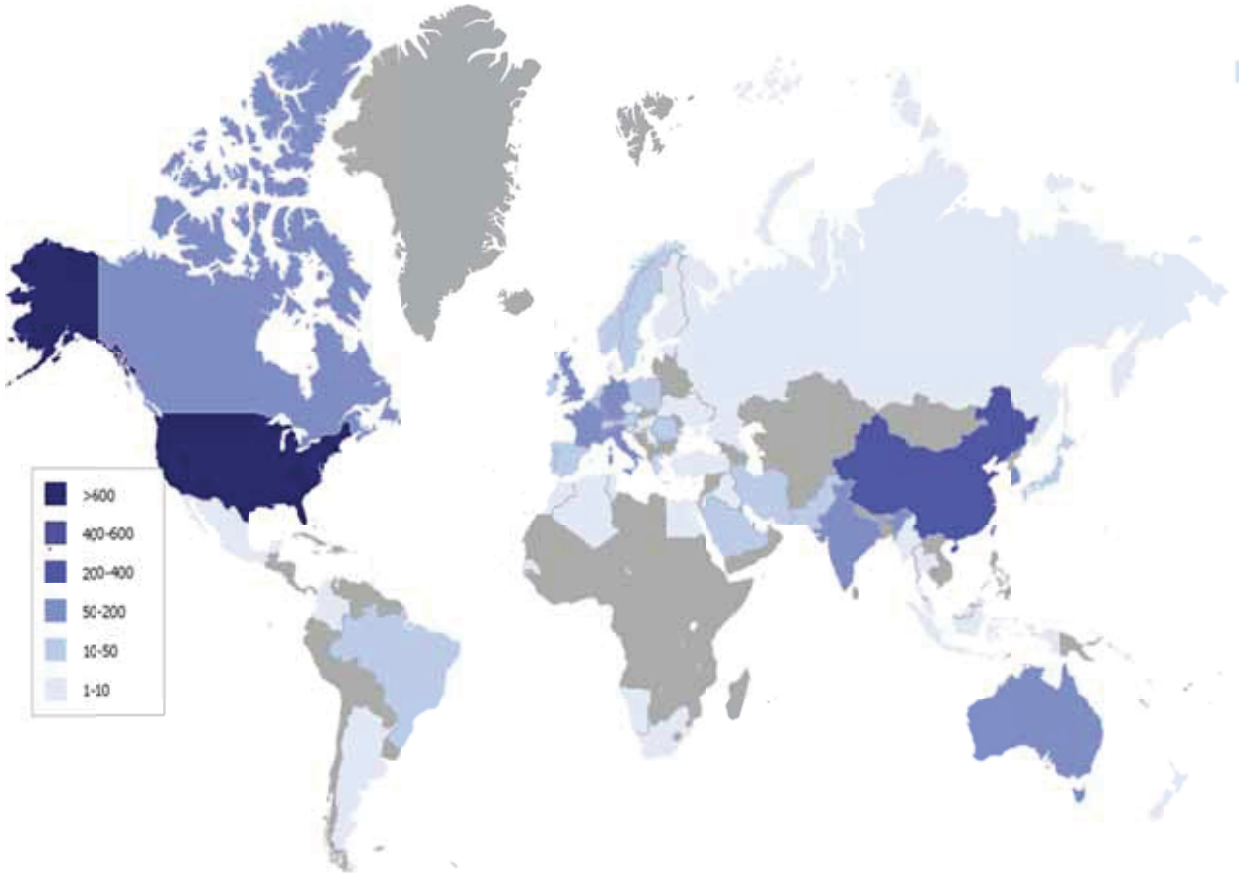


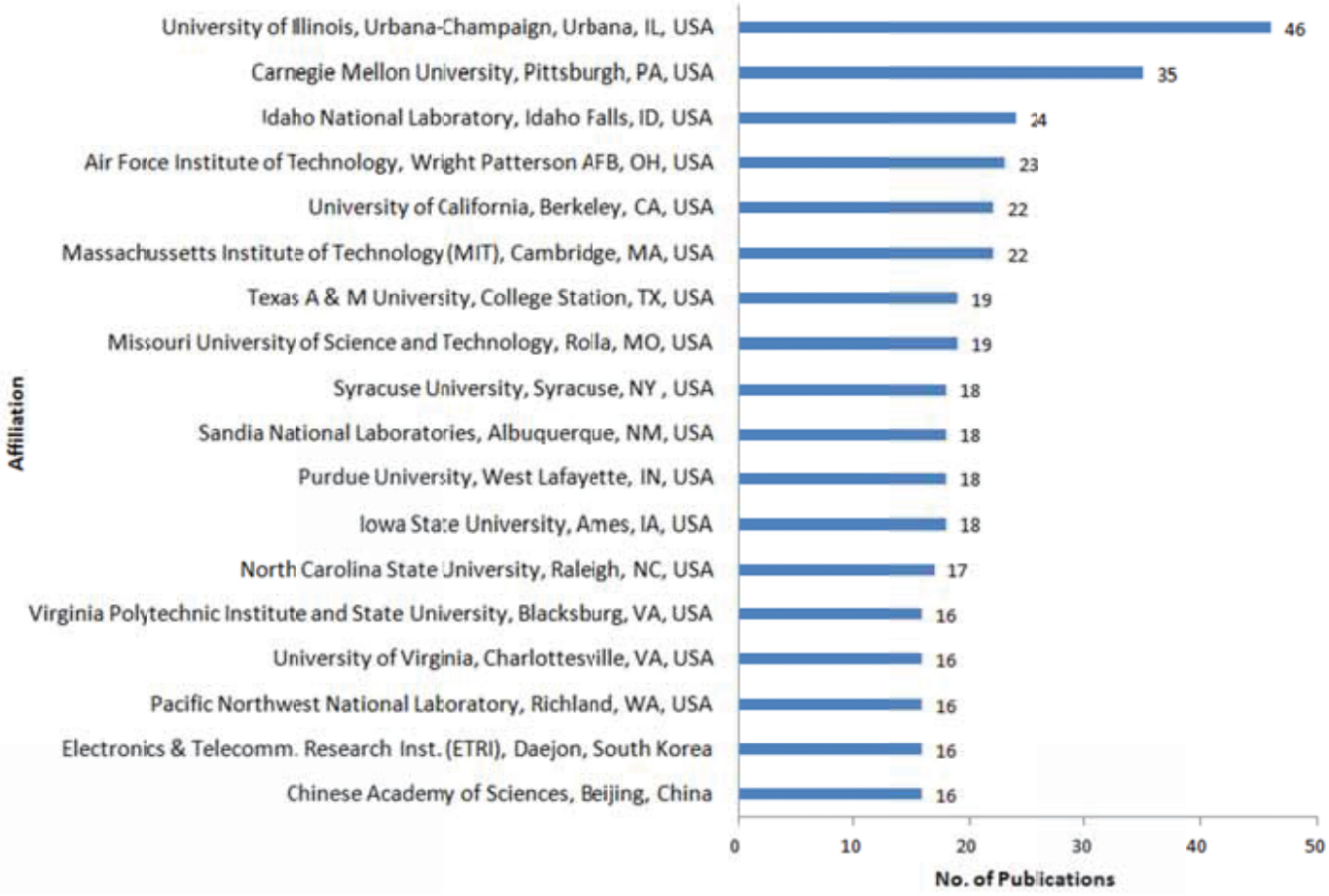
Figure 18. Master Dataset: Geographic Distribution, Numbers of Publications, 2003-2013

3.3.2 Top Organizations

[b] The U.S. and Chinese shares here may be compared to the most recent data on academic outputs published by the U.S. National Science Board at http://www.nsf.gov/statistics/seind12/pdf/c05.pdf In these data, for 2009, the U.S. accounts for 26% of *all* science and engineering publications, and China, in second place, held a 9% share of the world total. Annual growth rates in Asia were high, however: overall, Chinese production has increased 16.8% between 2008 and 2009.

The top affiliates in the database (with 16 or more publications in the database) are shown in Figure 19. They demonstrate the strong presence of academic institutions in the United States and China, and especially strong performance from the University of Illinois at Urbana-Champaign and Carnegie Mellon University. The strong presence of academic institutions is unsurprising, given the data sources (scientific and technical databases) and the reported immaturity of the technology (i.e., it is still at the research phase of maturity). In this category, universities such as the University of Illinois, the University of California, and the Massachusetts Institute of Technology are apparent, but there are also some smaller, specialist academic institutions (Syracuse, Missouri University of Science & Technology, Iowa State). The interest of governments and the importance CPS to national security is seen through the participation of government laboratories (Idaho National Lab, Sandia, Pacific Northwest National Lab).

Figure 19. Master Dataset: Top Affiliations (≥16 Publications)



3.3.2.1 Top Organizations by Type

To illustrate the types of organizations publishing in this field, we classified the affiliations in the database according to the following categories:

- Academic: colleges, universities, research academies such as the Chinese Academy of Sciences.
- Commercial: corporations, mostly private sector but also some utilities that may be public sector.
- Research and Technology Organizations (RTOs): research institutes which, although they may receive government funding or perform corporate contract research, are largely independent agencies.
- Military: military research labs, defence departments, and also academic institutions which provide training to military personnel (e.g., Air Force Institute of Technology, Royal Military College).
- Government: government departments (national or sub-national), other than military.
- Canadian: all affiliates located in Canada; these are also cross-referenced in the other classifications.

A breakdown of affiliations by organizational type appears in Figure 20.

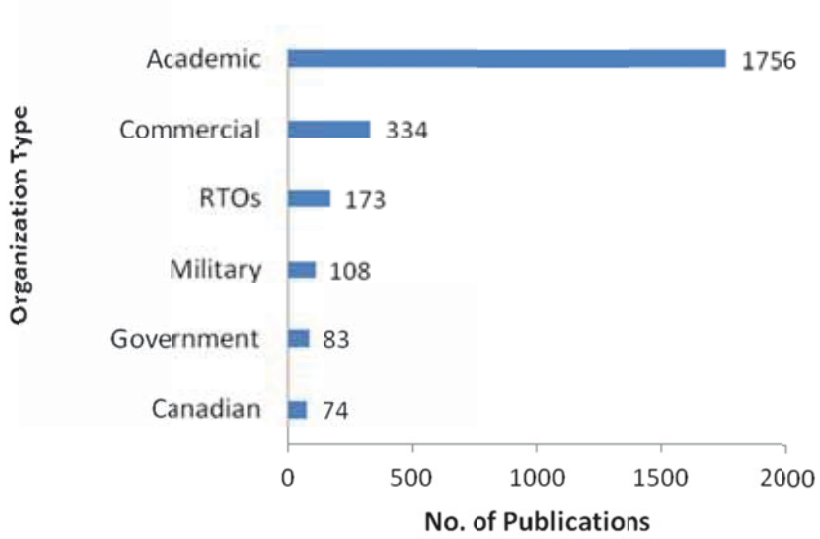


Figure 20. Master Dataset: Affiliation Types, 2003-2013

Although no standardized value exists that expresses a "normal" participation rate for commercial, governmental, or other organizational types in scientific and technical databases (academic participation is clearly to be expected), commercial publications (334 titles, or 15%) seems relatively high in number. This may be a function of the high degree of ownership/interest of private companies in the area of cyber-physical systems.[c]

[c] As a note of possible interest, the proportion of private ownership of IT infrastructure related to cyber-physical systems is cited as a particular challenge for security in this area in a recent article in the *MIT Technology Review*; this was also referenced in the 2013 State of the Union address which called for increased cooperation between government and private companies. See: Talbot D. Obama announces plans to shore up U.S. cyber defenses. *MIT Technology Review*. February 13, 2013. Accessed at http://www.technologyreview.com/news/511251/obama-announces-plan-to-shore-up-us-cyber-defenses/

A majority of publications which have been classified as commercial in the Master dataset, however, are co-publications with other types of entity, chiefly academic. Figure 21 illustrates the degree of overlap between affiliation types: in this cluster graph, co-occurrences between the major classifications are shown on the overlapping nodes. Each yellow dot represents a single publication and the total number for each major classification appears next to the label name. As seen here, 193 of 334 "commercial" articles are in fact co-publications.

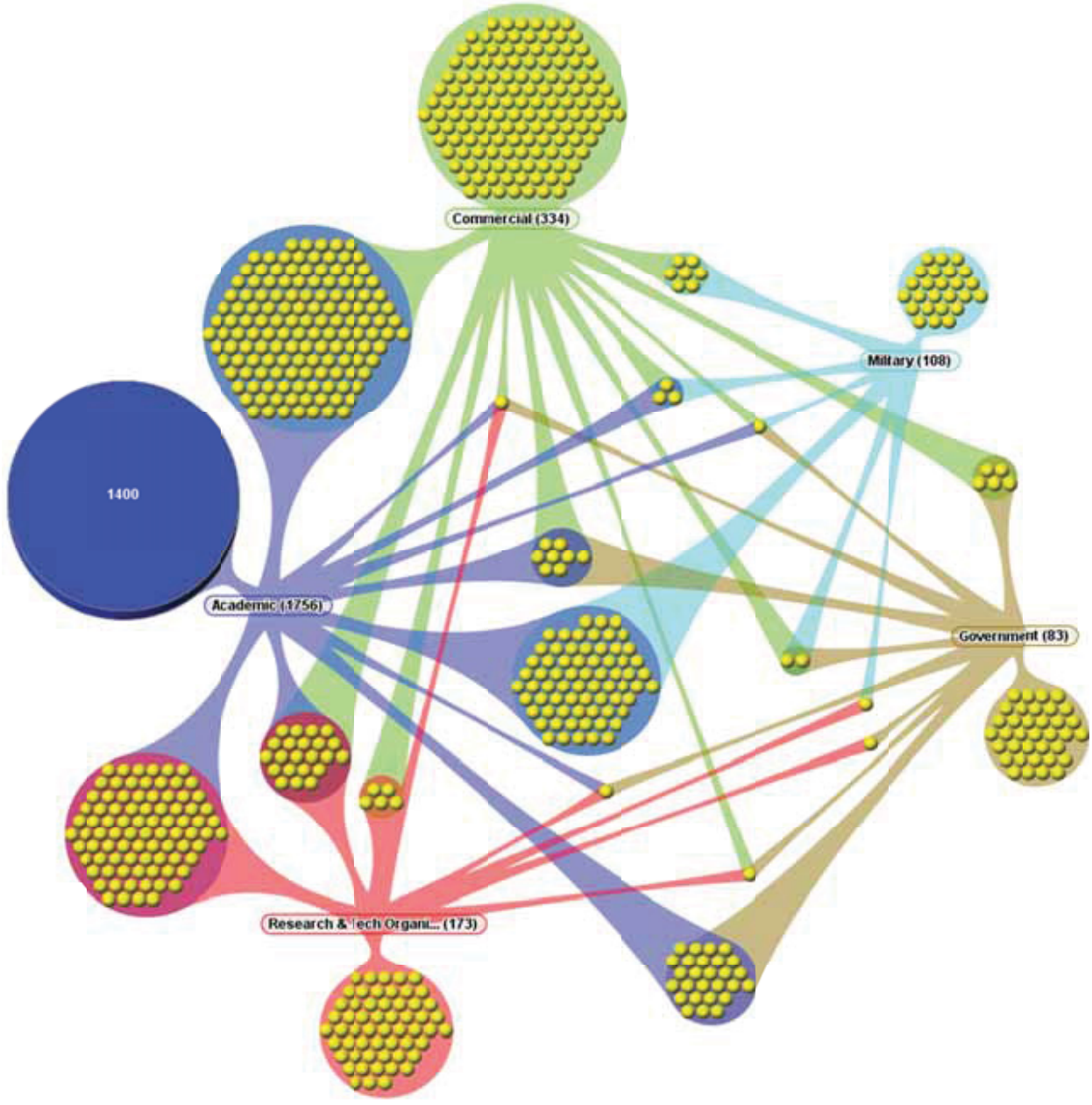


Figure 21. Master Dataset: Co-Publication by Type of Organization

The top players by category appear in Table 3.

Table 3. Master Dataset: Top Organizations

Category	Top 5 Organizations (# Publications)
Academic	• University of Illinois, Urbana Champaign, IL, USA (48) • Carnegie Mellon University, Pittsburgh, PA, USA (35) • Massachusetts Institute of Technology, Cambridge, MA, USA (22) • University of California, Berkeley, CA, USA (22) • Missouri University of Science & Technology, Rolla, MO, USA (19) • Texas A&M University, College Station, TX, USA (19)
Government	• Idaho National Laboratory, Idaho Falls, ID, USA (24) • Sandia National Laboratories, Albuquerque, NM, USA (18) • National Institute of Standards & Technology, Gaithersburg, MD, USA (5) • Department of Homeland Security, Washington, DC, USA (4) • State Grid Electric Power Research Institute, Nanjing, China (4)
RTOs	• Electronics & Telecommunications Research Inst.(ETRI), Daejeon, South Korea (18) • Royal Institute of Technology (KTH), Stockholm, Sweden (14) • Fraunhofer Inst.for Experimental Software Engineering, Kaiserslauten, Germany (8) • Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany (5) • ENEA – Italian Nat'l Agency for New Tech., Energy & the Environment, Rome, Italy (4) • Korea Atomic Energy Research Institute, Daejeon, South Korea (4) • Tecnalia, Zamudio, Spain (4)
Commercial	• Electricité de France (EDF), Paris, France (11) • CESI Ricerca, Milan, Italy (8) • MITRE Corporation, McLean, VA, USA (7) • SRI International, Menlo Park, CA, USA (7) • BBN Technologies (Raytheon), Cambridge, MA, USA (4) • IBM T.J. Watson Research Center, Hawthorne, NY, USA (4) • Siemens Corporation, Princeton, NJ (4) • Telcordia Technologies, Piscataway, NJ, USA (4)
Military [d]	• Air Force Institute of Technology, Wright Patterson AFB, OH, USA (23) • Air Force Research Laboratory, Rome, NY (14) • Air Force Research Laboratory, Wright Patterson AFB, OH, USA (12) • National University of Defense Technology, Changsha, China (8) • Naval Postgraduate School, Monterey, CA, USA (5) • Army Research Laboratory, Adelphi, MD, USA (5)
Canadian	• Ryerson University, Toronto, ON (11) • University of Victoria, BC (7) • University of British Columbia, Vancouver, BC (5) • University of New Brunswick, Fredericton, NB (5) • University of Ottawa, ON (5) • University of Waterloo, ON (5)

[d] Although no Canadian military institutions appear at the top, DRDC CORA (Ottawa) reports four publications in the Master dataset, DRDC Ottawa lists three, and DRDC Valcartier two. There are also two titles for Royal Military College in Kingston.

In Table 4 (academic organizations) and Table 5 (all other types), matrices were created of top organizations crossed with their publication counts for key subject groups. Cells in the matrix have been heat-mapped to indicate high (red) through low values (pale yellow).

Unsurprisingly, large institutions such as the University of Illinois demonstrate strengths in a number of areas. A degree of specialization is apparent for some other institutions, such as Texas A&M. Typically, where institutions specialize, it is in the area of the smart grid or sensor networks.

Table 4. Master Dataset: Areas of Expertise for Academic Organizations with ≥15 Publications

Total Records	Affiliation	Communications	Sensor networks	Wireless telecommunications	Public works and utilities	Intrusion detection	Models and modeling	Embedded systems	Smart grid and power systems	Network security	Cyber-physical systems	Network protocols	Software	Simulation	Critical infrastructure	Distributed computing	Military computing	Control systems	Hybrid, heterogeneous, interdep.	Safety
46	University of Illinois, Urbana-Champaign, IL	6	5	5	25	7	8	10	25	10	21	5	5	4	9	5	9	10	6	7
30	Carnegie Mellon University, Pittsburgh, PA	4	5		9	2	10	14	9	2	10	3	7	2	4	3	1	4	1	5
22	Massachusetts Institute of Technology, Cambridge, MA	4			3	1	5	6	3		5	1	1	1	2	5	1	3	4	2
22	University of California, Berkeley, CA	3	4	2	6	2	8	10	5	2	13	1	4	2	4	3	1	5	4	6
19	Missouri University of Science & Technology, Rolla, MO	5	7	2	10	2	8	8	8	1	15	1	4	4	4	4		1	3	1
19	Texas A & M University, College Station, TX	3	6	5	11	1	8	4	11	4	11	3	1	6	1	5		1	6	
18	Iowa State University, Ames, IA	4	3	3	11	1	6	4	11		4	1	2	5	2		1	5	1	8
18	Syracuse University, NY	4	9	9		2	4			3		4	2	2	3	6	3	1	1	
17	North Carolina State University, Raleigh, NC	7	6	7	4	3	2	6	4	4	3	1	1	1	2	4	3	1	2	
17	Purdue University, West Lafayette, IN	6	4	2	5	1	5	7	4	3	5	2	9	3	2	2	1	2	4	1
16	Chinese Academy of Sciences, Beijing, China	4	5	4	2	6	6	3	1	6	2	3	3	1		4	1	1	1	1
16	University of Virginia, Charlottesville, VA	4	6	5	4	1	5	5	3	2	3	3	4	2	4	2	5	3	4	2
16	Virginia Polytechnic Institute & State University, Blacksburg, VA	8	11	7	6	8	6	4	6	3	8	2	2	3	2	3	4	1	4	3

Total Records	Affiliation	Communications	Sensor networks	Wireless telecommunications	Public works and utilities	Intrusion detection	Models and modeling	Embedded systems	Smart grid and power systems	Network security	Cyber-physical systems	Network protocols	Software	Simulation	Critical infrastructure	Distributed computing	Military computing	Control systems	Hybrid, heterogeneous, interdep.	Safety
15	Anna University, Chennai, India	3	12	13	1	8	1	3	1			4		2		1	3	1	3	
15	Northwestern Polytechnic University, Xi'an, China	7	8	7	2	2	8	5	2	3	5	6	4	4	2			2	2	2
15	Zhejiang University, Hangzhou, China	6	10	8	3	2	4	4	3	1	4	2	1	6		2	1		2	

Table 5. Master Dataset, Non-Academic Organizations with ≥ 7 Publications, Top Subject Groups

Total Records	Affiliation	Communications	Sensor networks	Wireless telecommunications	Public works and utilities	Intrusion detection	Models and modeling	Embedded systems	Smart grid and power systems	Network security	Cyber-physical systems	Network protocols	Software	Simulation	Critical infrastructure	Distributed computing	Control systems	Hybrid, heterogeneous, interdep.	Safety	Military computing	SCADA systems
23	Air Force Institute of Technology, Wright Patterson AFB, OH	8	2	1	12	5	2	2	10	7		1	4	5	13	2	9	2	10	8	10
23	Idaho National Laboratory, Idaho Falls, OH	2	6	2	9	3	4	2	6	8	2		1	2	9	2	15	3	2	2	2
18	Sandia National Laboratories, Albuquerque, NM	5			9	1	7		6	2	2	1	2	7	6		8	3	1	6	3
16	Pacific Northwest National Laboratory, Richland, WA, USA	4	1		11		4	3	11	4	4	1	2	1		3	2	3	2		2
16	Electronics and Telecommunications Res. Institute (ETRI), DAEJEON, South Korea	8	5	4	5	3	4	8	4	3	9	5	3	3	1	2	2	2	2		2
14	Air Force Research Laboratory, Rome, NY	1	2		1	3	5	1	1	2	1		2	2	3	7	1		2	1	2
14	Royal Institute of Technology (KTH), Stockholm, Sweden	3	4	4	5	3	7	4	5	3	2	2	1		1	3	3	3	5		3
12	Air Force Research Laboratory, Wright-Patterson AFB, OH	5	3	2	6	3	1		5	1	1	2		4	6	2	3	1	4	5	4
11	Electricité de France (EDF), Paris, France	1	2	2	1	1	3		1	1	1				1		2	2	4		1
8	CESI RICERCA, Milan, Italy	8			8		1		8	1				1		1	3		4	1	4
8	Fraunhofer Inst. Experimental Software Eng., Kaiserslauten, Germany						6	6			1		7		2				7		
8	National University of Defense Technology, Changsha, China	3	4	4		1	2	1		2	2	2		4	1	4		3			
7	MITRE Corporation, McLean, VA	1			1		2	1	1	1	1			2						1	
7	SRI International, Menlo Park, CA	2			2	1	3	4	1		5		3		4	1	1	1	2	2	

3.3.3 Co-Publication

Co-publication between players is common in this dataset, but usually only among organizations with less than five publications. For these players, it is common that one or two instances of collaboration are reported. High-volume collaborations for high-publishing institutions are few.

Co-publications for organizations with at least five publications *and* at least two collaborations appear in Figure 22. In this view, the size of the bubble is relative to the total number of publications in the database for that organization. The number on the connecting line between labels indicates the actual number of co-publications.

The red clusters at the top of Figure 22 shows certain patterns of organizational collaboration by type (Air Force to Air Force, for instance), as well as geographic clusters (an Ohio cluster linking Wright Patterson Air Force Base to Ohio State University; the Air Force Research Lab in Rome New York with Syracuse University). A turquoise cluster linking mainly academic organizations also demonstrates the centrality of the Idaho National Laboratory (INL) in research networks: INL performs research for the U.S. Department of Energy and is active in studies of the electrical grid and nuclear power.

Most instances of co-publication shown in this graphic are between academic institutions. For some institutions which are very active overall, such as the University of Illinois, there are very few instances of collaboration.

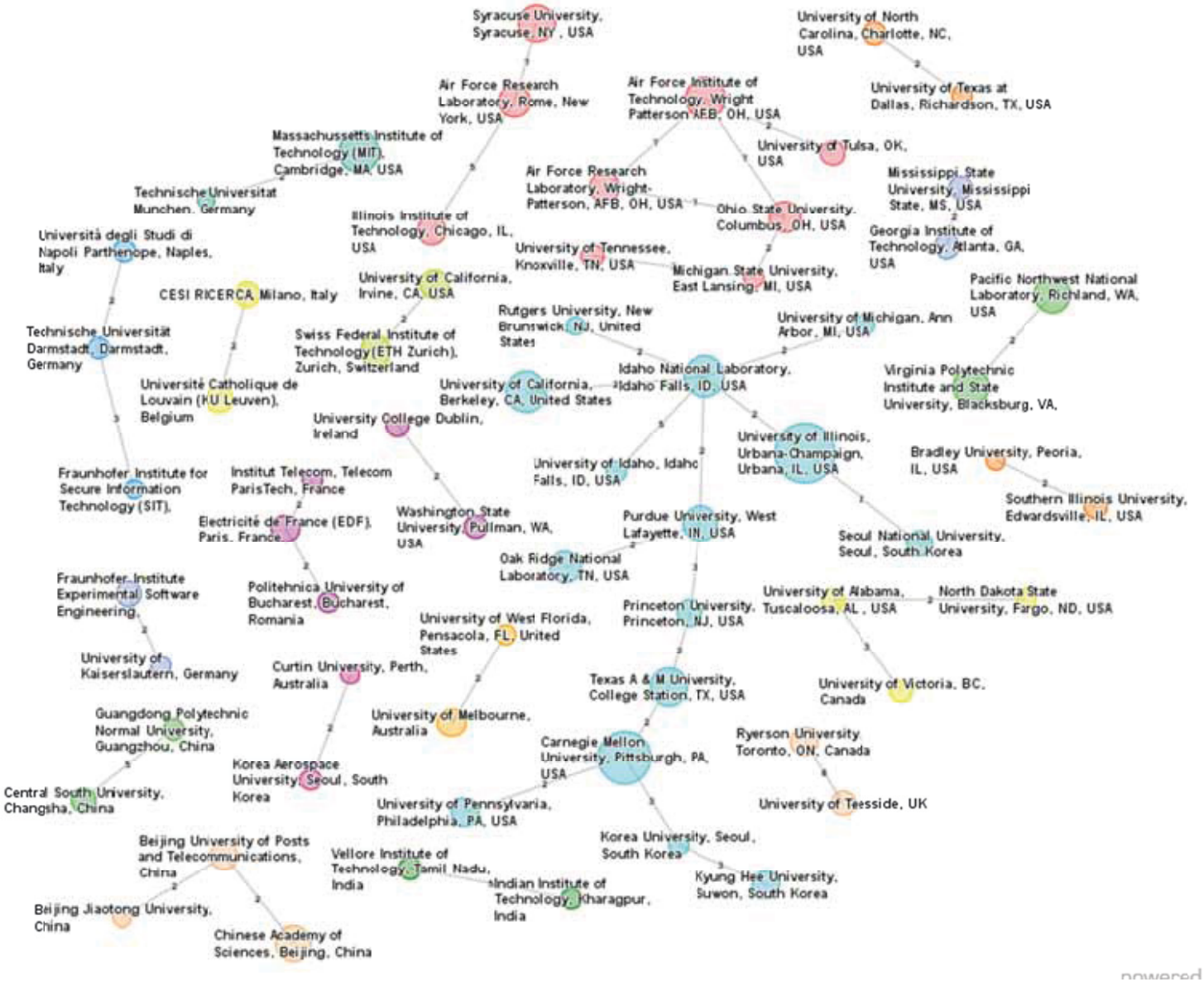


Figure 22. Master Dataset: Key Players: ≥5 Publications and ≥2 Co-Publications

3.3.4 Top Authors

Top authors (8 or more publications) found in the Master dataset, and a brief statement as to their research interests, are shown below in Table 6. Where active websites could be determined for these authors, URLs are embedded on the author name.

Table 6. Master Dataset: Top Authors

Author	Institution	Topics	# Articles
Govindarasu, M.	Iowa State University, Ames, IA, USA	Cybersecurity, real time embedded systems, smart grid, defence	11
Cheung, R.	Ryerson University, Toronto, ON, Canada	Power system operations & engineering	10
Das, S. K.	University of Texas, Arlington, TX, USA	Wireless mobility, sensor networks	10
Sinopoli, B.	Carnegie Mellon University, Pittsburgh, PA, USA	Networked embedded control systems	9
Mander, T. (student)	Ryerson University, ON & Teeside University, UK	Security architecture, routing, P2P	9
Dondossola, G.	CESI Ricerca, Milan, Italy	Security for power control systems	8
Dimitriou, T.	Athens Information Technology, Greece	Optimization and probabilistic algorithms for sensor nets	8
Muraleedharan, R.	formerly Syracuse University, NY, USA; now Glassboro University, NJ, USA	Behavioural studies/computer engineering	8
Nilsson, D. K.	Chalmers University of Technology, Gothenburg, Sweden	Automotive networks, embedded systems	8
Osadciw, L. A.	Syracuse University, NY, USA	Signal processing, Bayesian networks, routing	8

3.3.5 Top Authors Cited (External to Master Dataset)

Although not all records in the Master dataset include information on citations to other works, 74% of the dataset articles (mostly those sourced from Scopus) do include such references. In Table 7, the top authors *cited* by articles in our database are listed. It should be noted that the subject matter of their publications may not be directly on point. The column on the far right of the table indicates the representation, if any, of these same authors in the Master dataset.

Table 7. Top Authors Cited by Authors in Master Dataset

Author	Affiliation	Research interests	# articles in Master dataset citing this author	#articles by this author in Master dataset
Perrig, A.	Carnegie Mellon University, Pittsburgh, PA (director of CyLab) and formerly ETH Zürich, Switzerland	Network and systems security for mobile computing and sensor networks	265	6
Stankovic, J.	University of Virginia, Charlottesville, VA	Real-time computing, cyber-physical systems, wireless sensor networks, and wireless energy and health applications.	205	5
Wagner, D.	University of California, Berkeley, CA	Computer security, especially of large-scale systems and networks; smartphone and wireless security; applied cryptography	186	0
Zhang, Y.	Microsoft Research, Beijing Labs; formerly HRL Labs of Malibu, CA and various U.S. academic institutions	Intrusion detection in WSNs; mobile and satellite networks	175[e]	1
Culler, D.E.	University of California, Berkeley, CA	Network architectures for energy reduction, wireless embedded systems, parallel computing	159	0
Ning, P.	North Carolina State University, Raleigh, NC – currently on sabbatical with Samsung Mobile	Cloud computing security, wireless security, post-detection analysis of intrusion alerts	132	6
Akyildiz, I. F	Georgia Institute of Technology, Atlanta, GA	Wireless networking; modeling, analysis and control of complex multi-scale data networks	130	2

[e] Multiple authors with the name Y. Zhang appear in both the Master dataset authors field and the cited authors field, and it is not clear how many separate individuals are linked to this number. Yongguang Zhang of Microsoft Research appears to be the key author here.

Author	Affiliation	Research interests	# articles in Master dataset citing this author	#articles by this author in Master dataset
Karlof, C.	Formerly University of California, Berkeley, CA (Ph.D. student), now a private security architect and software engineer	Full stack software development, mobile security and privacy	127	0
Liu, Y.	University of South Florida, Tampa, FL; formerly a Ph.D. student at North Carolina State University, Raleigh, NC (under P. Ning, above)	Cybersecurity of wireless and CPS, especially smart grid	114	0
Su, W.	Naval Postgraduate School, Monterey, CA; former student of Ian Akyildiz (Georgia), above	Sensor, satellite, and distributed networks; QoS; cybersecurity	112	0

4 MODELING AND SIMULATION

A subset of articles related to modeling and simulation was created by extracting all records from the Master dataset which contain the terms *model* OR simulat** in the title, abstract, or keyword fields. This resulted in a subset of 1,004 titles. The top 300 terms cover 96% of the (subset) database content. The subject groupings used in the subset were the same as for the Master dataset . In the subset, the subject groups cover 97% of content.

4.1 Major Research Topics

4.1.1 Top Subject Groups

Unsurprisingly, given the method of creation for the subset, a review of the top subject shows that, compared to the Master data, *Models and modeling* and *Simulation* have risen higher in the rankings, at first and fifth spots, respectively. Sensors, networks and communications topics continue to demonstrate strong presence in the data.

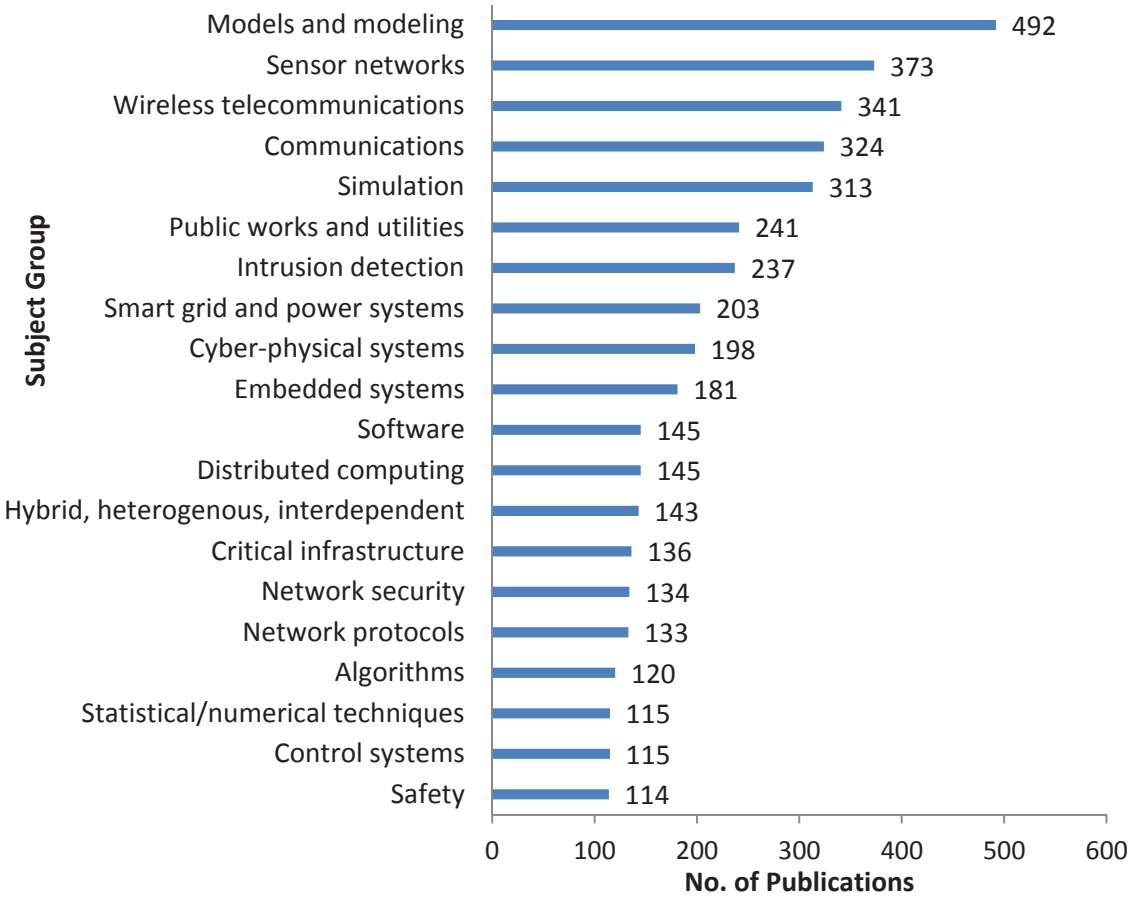


Figure 23. M&S Subset: Top Subject Terms Ranked by Number of Publications

Closer inspection of the temporal distribution of publishing activity for these subject groups shows that the bulk of activity occurred in the last half of the decade, however, as shown in Figure 24.

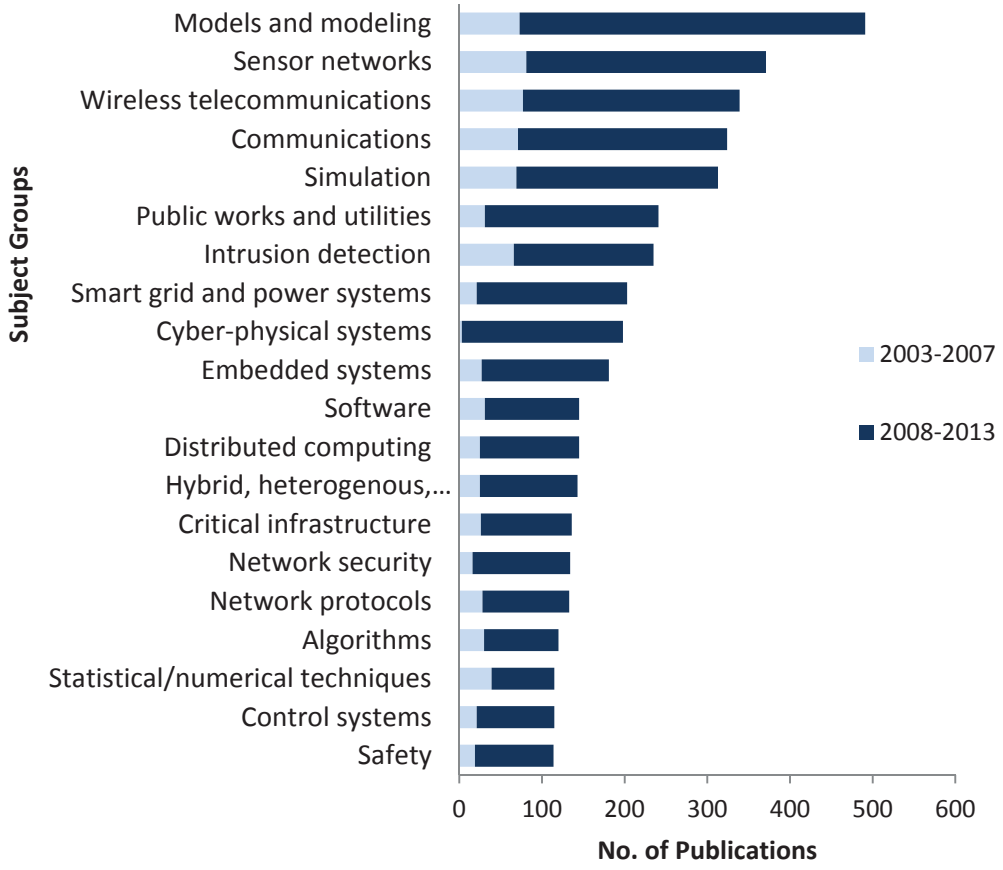


Figure 24. M&S Subset: Publications for Top Subject Groups, Early vs. Late

4.1.2 Topical Correlations

To see how topical clusters and correlations in the subset may also have been affected by changes over time, three views of the top 300 terms in the subset were prepared: a composite picture of the entire period (2003 to 2013); a snapshot of the early period (2003-2007); and a view of the later period (2008-2013). The three maps corresponding to these time slices are included as Figures E-H in Appendix 1 to this report.

In the M&S correlation map for all years, as seen the excerpt below (Figure 25), there are several tightly linked clusters on topics such as safety, reliability, and risk assessment, suggesting these are especially important areas of application for modeling and simulation. These considerations are, of course, critical to operation of infrastructure such as power and water systems. As a side note of possible interest, and as further evidence of the importance of safety and reliability to critical infrastructure, one recent article in *MIT Technology Review* suggested that electrical, water, and transportation systems have, until recently, downplayed cybersecurity in favour of reliability, in spite of increasing attacks. This lack of attention and the fact that many applications which were originally standalone are now networked has made these systems more vulnerable to cyberattacks. The article also quotes a researcher from the University of Illinois at Urbana-Champaign as stating "… the major companies are backfilling very rapidly…but closing every weak point in a complex mix of control software and infrastructure companies' computer networks is challenging." [21]

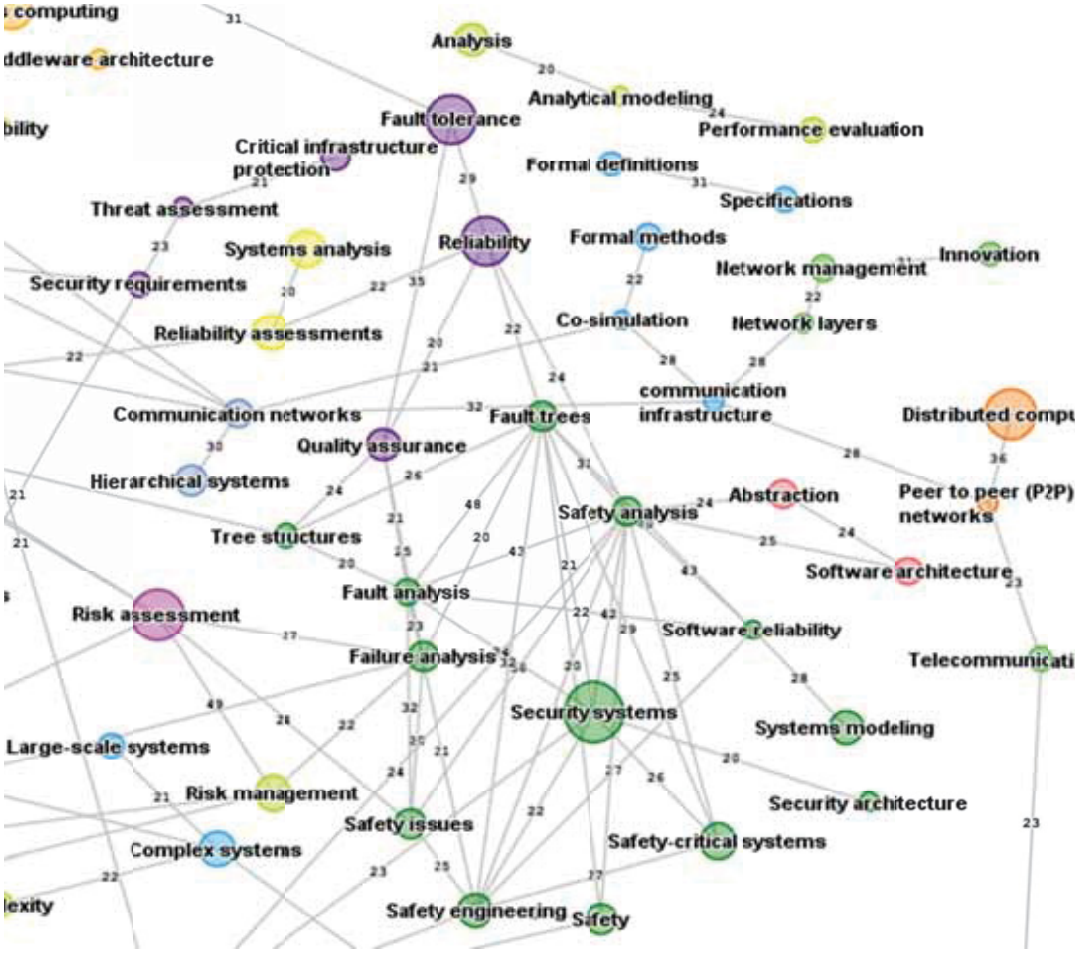


Figure 25. M&S Subset, 2003-2013: Safety and Risk Clusters, ≥20% Correlation

In another excerpt from the main M&S map, specific models and security-related modeling methods are apparent; for instance, *Markov processes* are linked to *Survivability*, *Stochastic models* and *Agent-based systems* to *Systems of systems*, *Hardware-software* to modeling *Testbeds*, and so on.

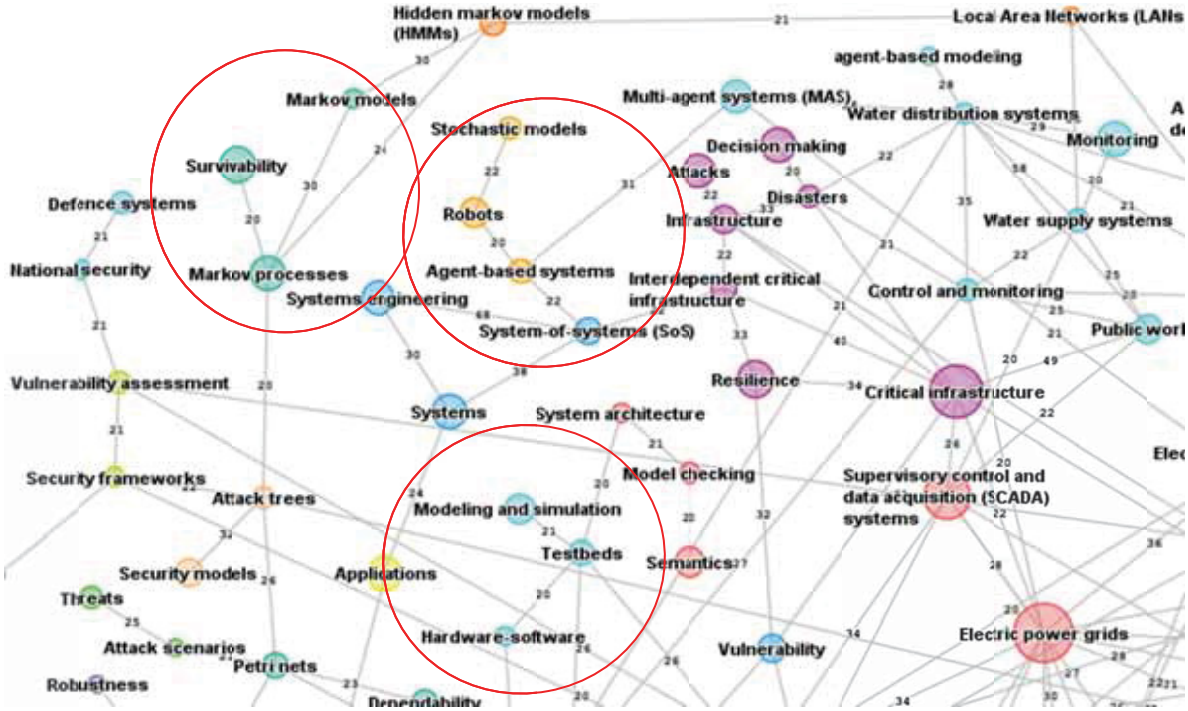


Figure 26. M&S Subset, 2003-2013: Various Modeling Clusters, ≥20 Correlations

For the early years of the M&S subset (2003-2007, Appendix 1, Figure G), it is apparent that much of the attention in the data is directed to wireless sensor networks, network architecture, intrusion detection, denial of service, routing, authentication, and other "traditional" cybersecurity topics. For example, in the excerpted view below (Figure 27), a large node for *Simulation* is coupled with *Security, Internet, Quality of service, Information security management systems*, and *Wireless telecommunication systems*, suggesting that most simulation activity at this early stage was related to network traffic and security and WSNs.

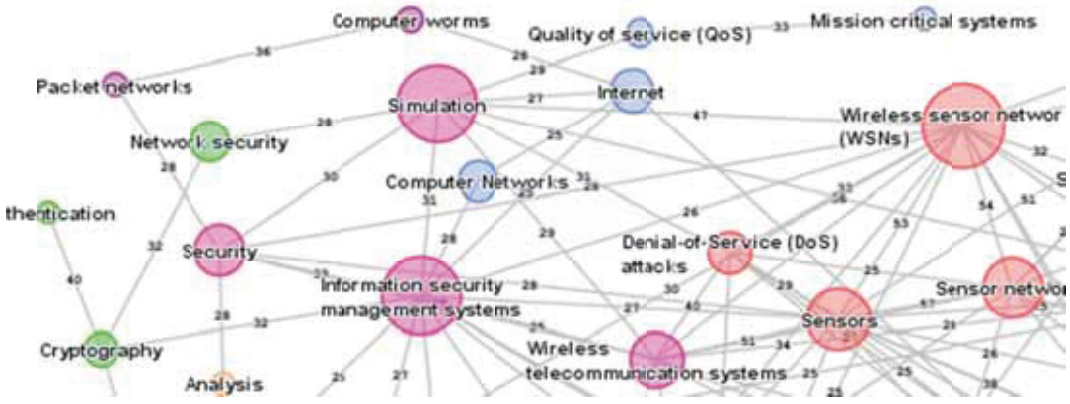


Figure 27. M&S Subset, 2003-2007: Simulation and Telecommunications, ≥20 Correlations, ≥5 Publications

In Figure 28, also extracted from the map for 2003-2007, a large node for *Mathematical models* is linked to *Network protocols.* Outside of the visible portion of this excerpt, there is also a connecting line to *Information security management systems* (top left, as seen in Figure 27, with a correlation of 31%). Thus, for the period 2003 to 2007, there appears to be a high degree of correlation overall between M&S and the network and communications aspects of cyber-physical systems.

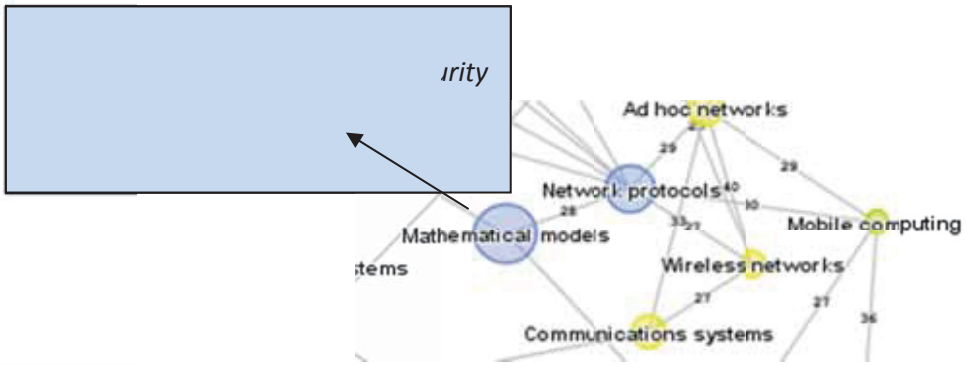


Figure 28. M&S Subset, 2003-2007: Simulation and Telecommunications, ≥20 Correlations, ≥5 Publications

Shifting focus to the period 2008-2013 (Appendix 1, Figure H), we see a greater diversity of topics and more emphasis on different types of cyber-systems; relative to the still-apparent WSN and network nodes, the size of other bubbles, such as those for *Embedded systems*, *Smart grids*, and *Critical infrastructure* has increased markedly over the early data. In an excerpted view (Figure 29), a large node with the generic caption *Modeling* is shown linked to both *Embedded systems* and *Cyber-physical security systems*, each at a correlation rate of 31%.

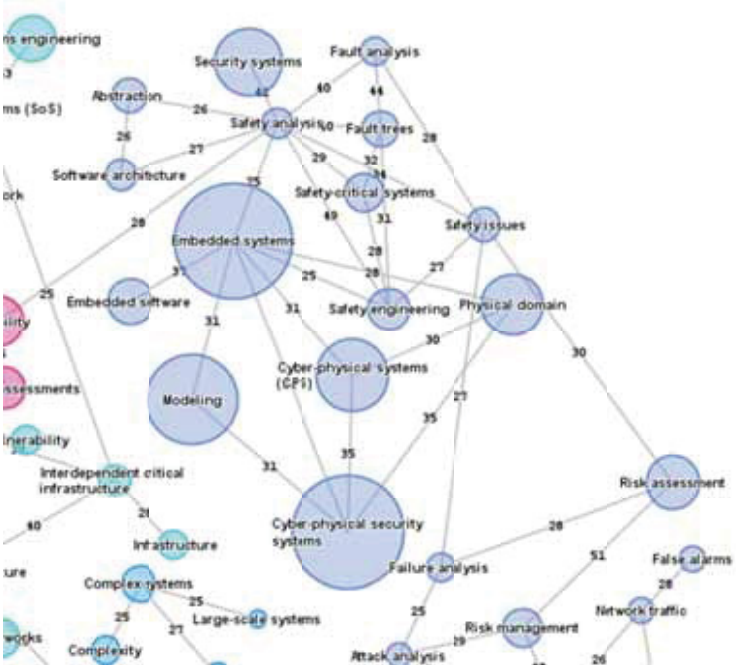


Figure 29. M&S Subset, 2008-2013: Modeling, Embedded systems, and Cyber-Physical security systems

Elsewhere in the map for 2008-2013, specific types of modeling are coupled to specific types of system or attributes. For instance, Markov models are shown linked to local area networks/electrical grid as well as survivability (Figure 30).

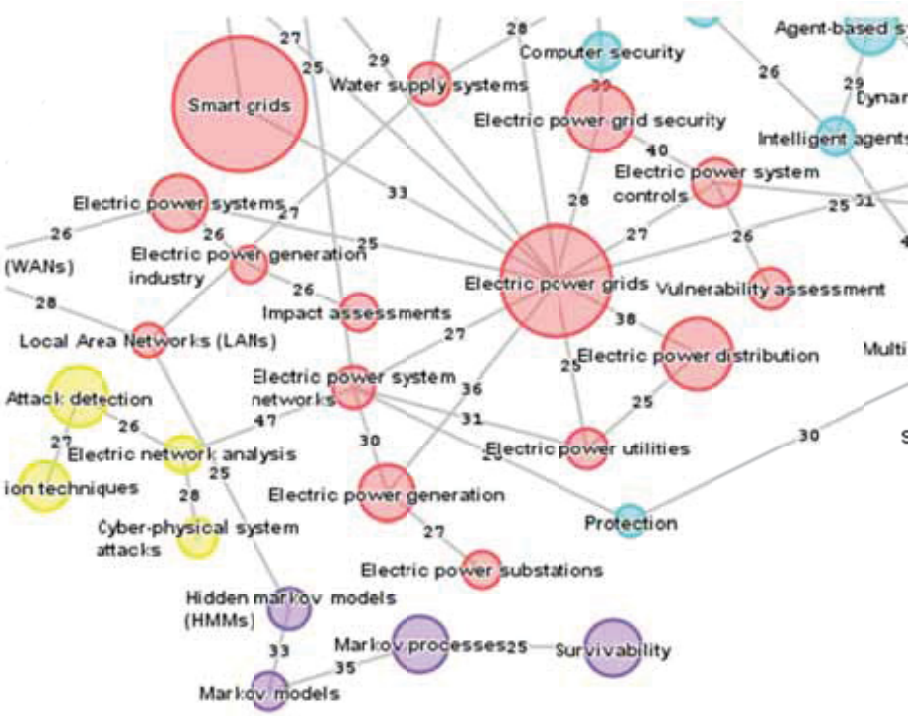


Figure 30. M&S Subset, 2008-2013: Markov processes, Smart grid, Survivability

Compared to the earlier time period, more diverse threat-defence approaches are also present in the data for 2008-2013: there are references to artificial immune systems, attack trees/ models, intelligent and/or agent-based systems, for instance, presumably to address the ever-expanding complexities of cybersecurity. Many of these defensive techniques are still shown linked to network and communications architectures, but risk assessments are also implicated. In Figure 31, for example, *Attack models* and *Attack analysis* correlate with *Risk management* and *Process control systems* as well as *Network traffic*.

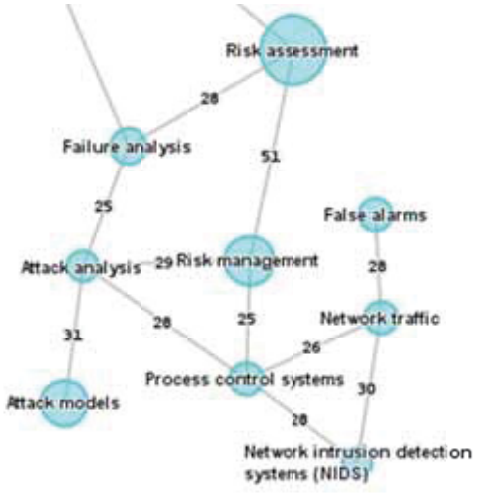


Figure 31. M&S Subset, 2008-2013: Attack models, Risk management and Process controls

4.2 Emerging Research Trends

For the Modeling and Simulation data, the overall pattern for publications over time shows an overall dramatic growth for the last decade. In this regard, the M&S subset closely resembles that of the Master set. However, once again, there is a decline in publications at the end of the period.

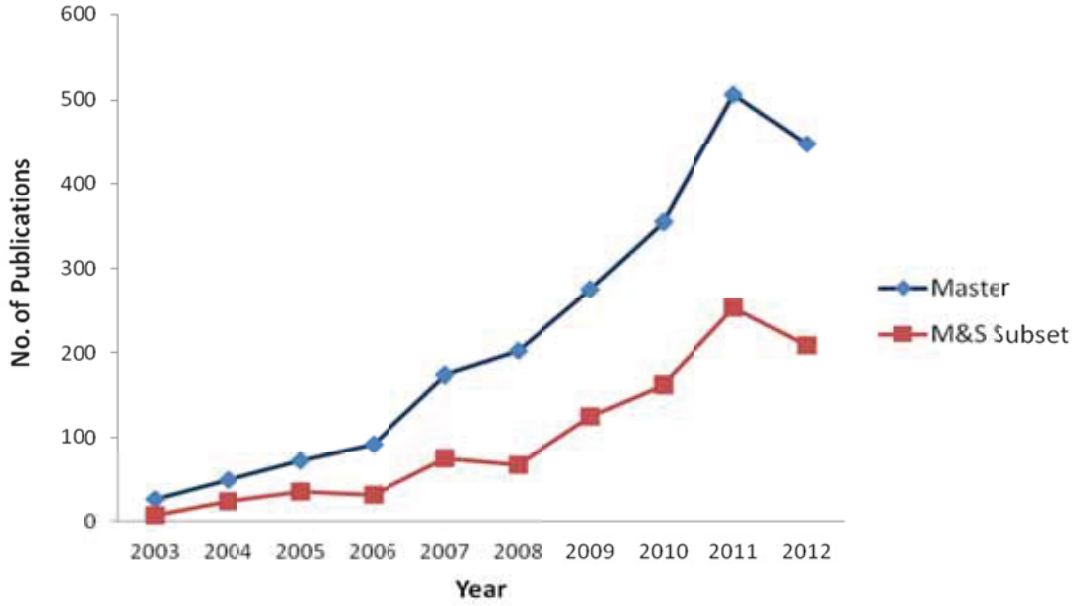


Figure 32. Comparison of Publication Activity, 2003-2012, Master vs. M&S Subset

As with the Master data, it is likely that certain high-volume groups in the area of networking and communications contribute to the decline at the end of the period:

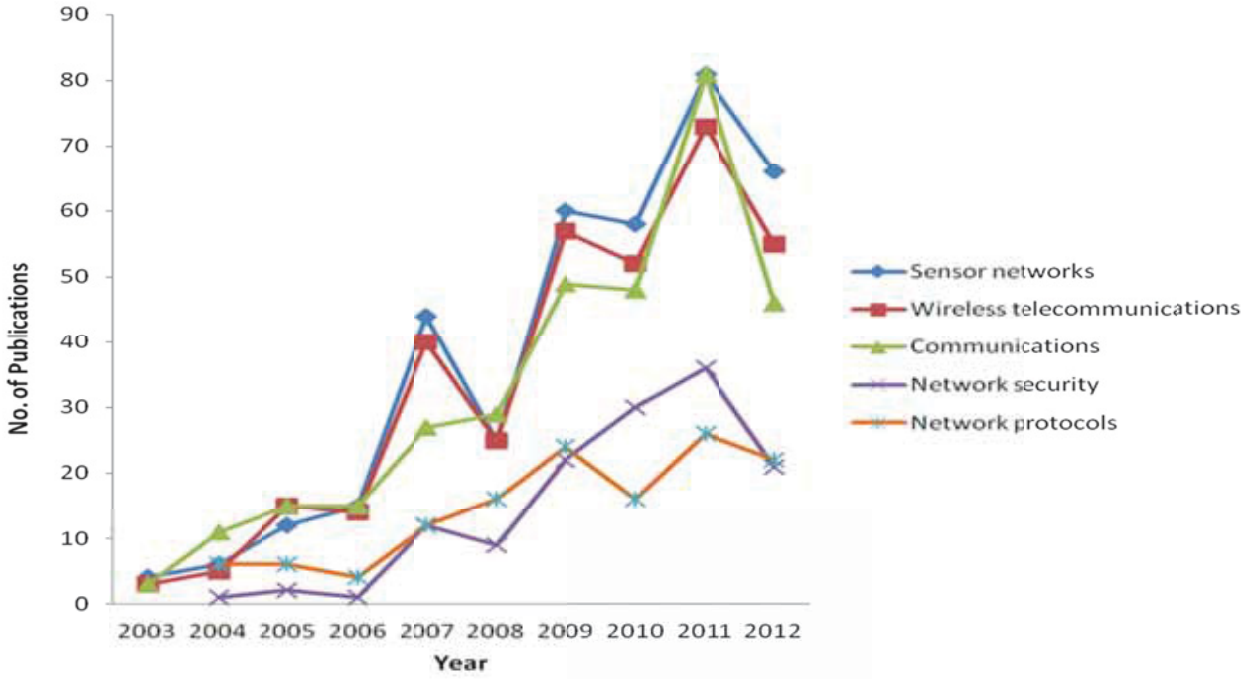


Figure 33. M&S Subset, Selected Groups with Declining Levels of Publication Activity, 2003-2012

However, as with the Master set, certain subject groups defied the downward trend at the end of the period and showed rising or stable activity from 2010 to 2012. In the sections which follow, we review performance measures for subject groups by genre, showing the top-ranked items, those with rising publication trajectories, and normalized rates of research/publication interest. Taken together, these analyses suggest topical areas strongest performance/emergence in the M&S dataset.

4.2.1 Methods or Techniques

As was the case for the top subject groups in the Master dataset for the genre *Methods or Techniques* (Figure 7), *Models and modeling, Simulation*, and *Algorithms* here rank 1-3 by volume. Several other groups, such as *Prediction, Probability*, and *Formal methods/verification* improve in standing in the current analysis, and groups for *Semantics, Game theory, Markov processes* , and *Trees (graph, attack, fault, threat)* appear in this list, but were not found at the top of the Master rankings.

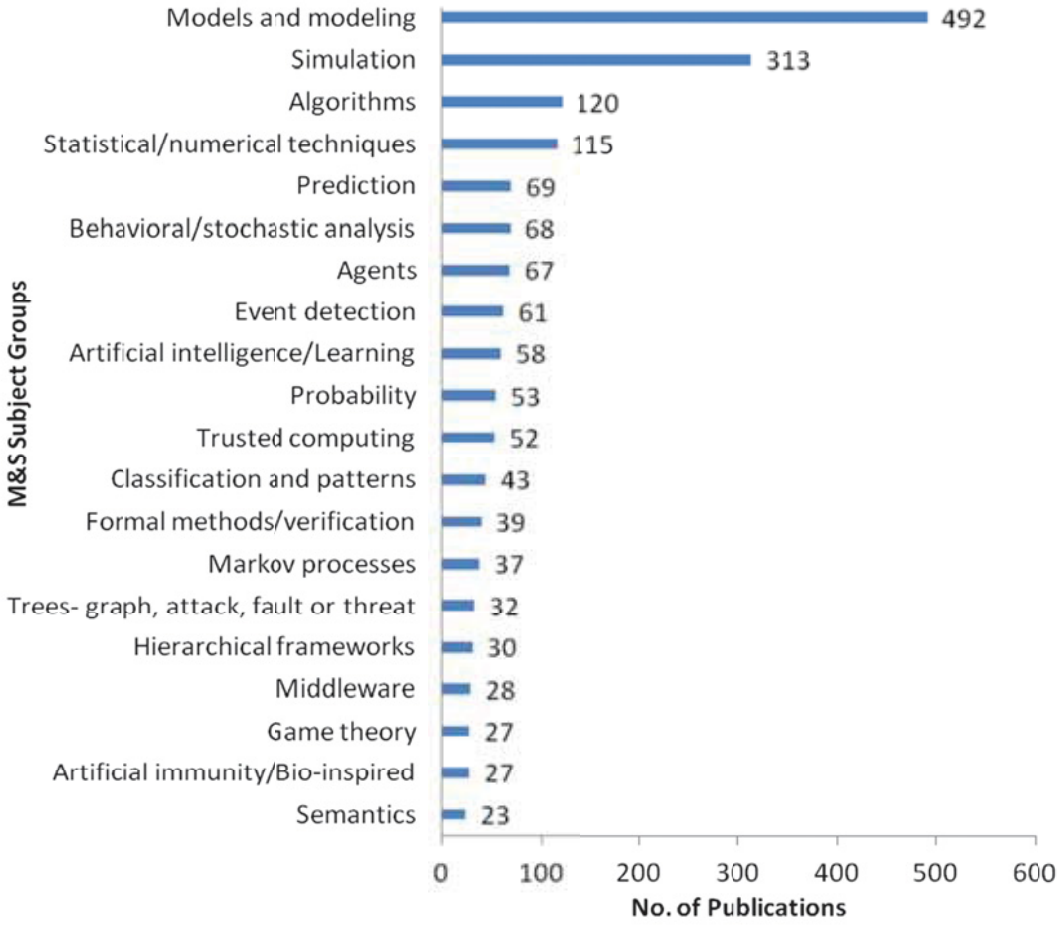


Figure 34. M&S Subset: Top Subject Groups, Methods or Techniques, 2003-2013

Figure 35 portrays subject groups in the category *Methods or Techniques* which show an increase in publication at the end of the period studied. Although some groups demonstrate somewhat erratic performance, certain groups, such as *Models and modeling*, *Algorithms* and *Behavioral/stochastic analysis* rise markedly post-2008. At a slightly lower rate of increase and with smaller absolute numbers, we also see *Artificial intelligence/Learning*, *Trusted computing*, and *Formal methods/verification*.

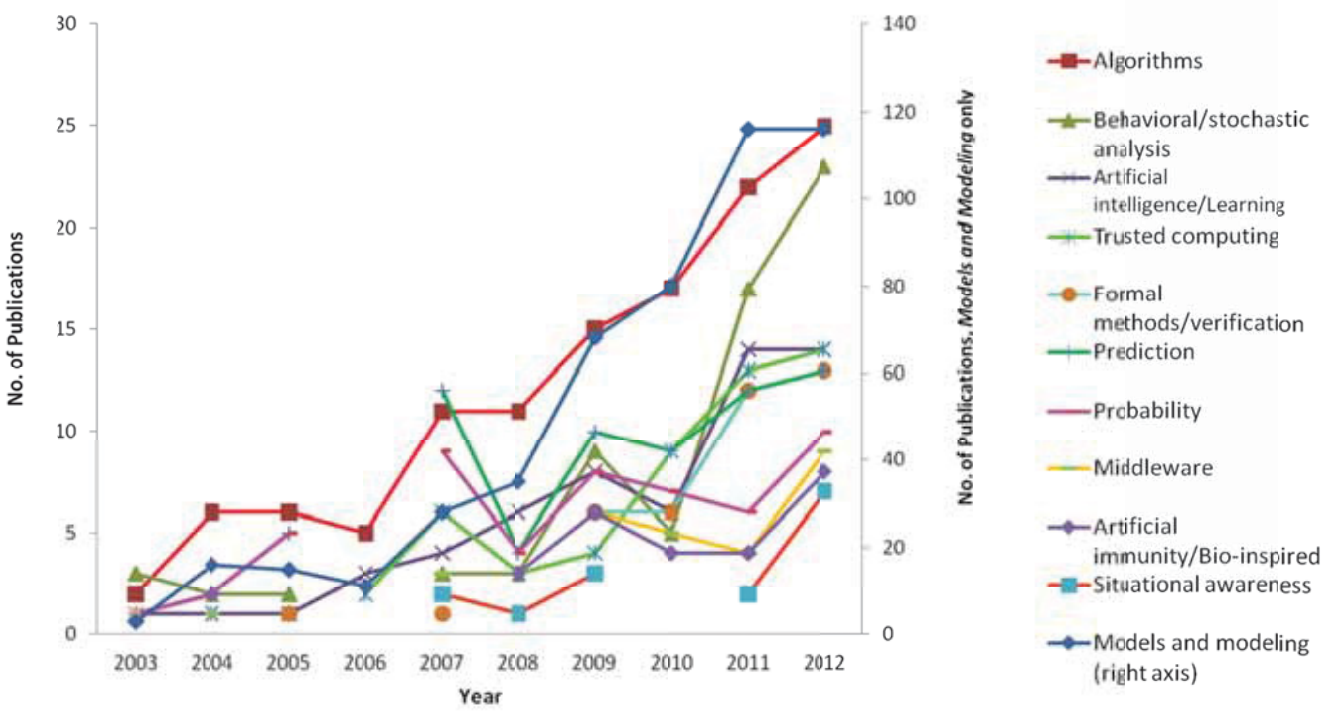


Figure 35. M&S Subset: Methods or Techniques with Rising Numbers of Publications, 2003-2012

Several of subjects with rising publication numbers also show stronger (normalized) velocity. In Figure 36, for instance, positive values are seen for *Models and modeling, Formal methods/verification, Trusted computing, Artificial intelligence/learning, Algorithms, Prediction*, and *Middleware*. Relative to these groups, some other groups such as *Behavioral/stochastic analysis, Probability*, and *Artificial immunity/Bio-inspired* demonstrated weaker smaller increases for the decade, even if actual publication counts in Figure 35 were shown to be ascendant most recently.

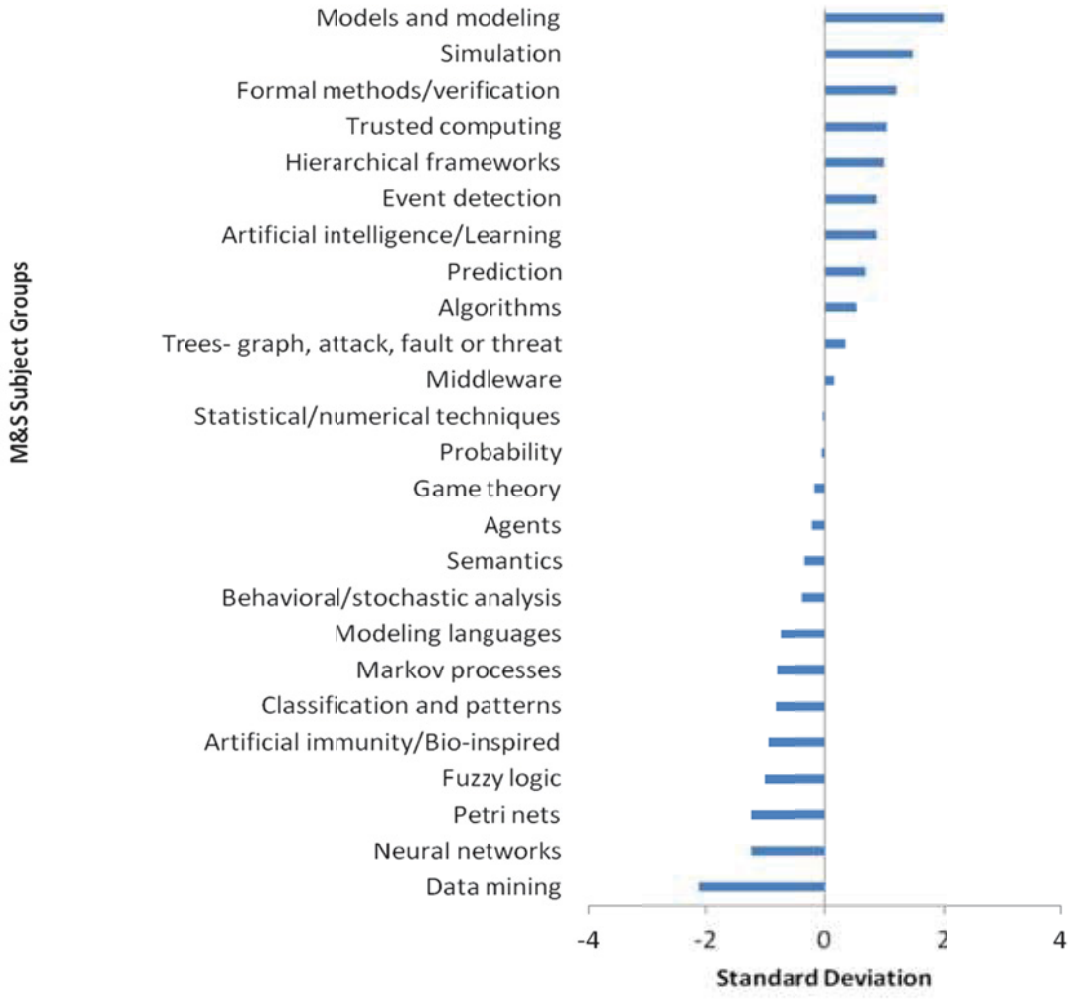


Figure 36. M&S Subset: Methods or Techniques: Relative Rate of Research Interest, 2003-2012

4.2.2 Features or Attributes

Figure 37 shows publication counts for the top M&S subset subject groups in the genre *Features or Attributes*. In this instance, the top three labels remain in the same order as was seen in the Master dataset (Figure 8). Most of the same groups appear on the list for both Master and Subset, although *Privacy* (22 items, not shown here) has dropped off the "top" list for the M&S subset.

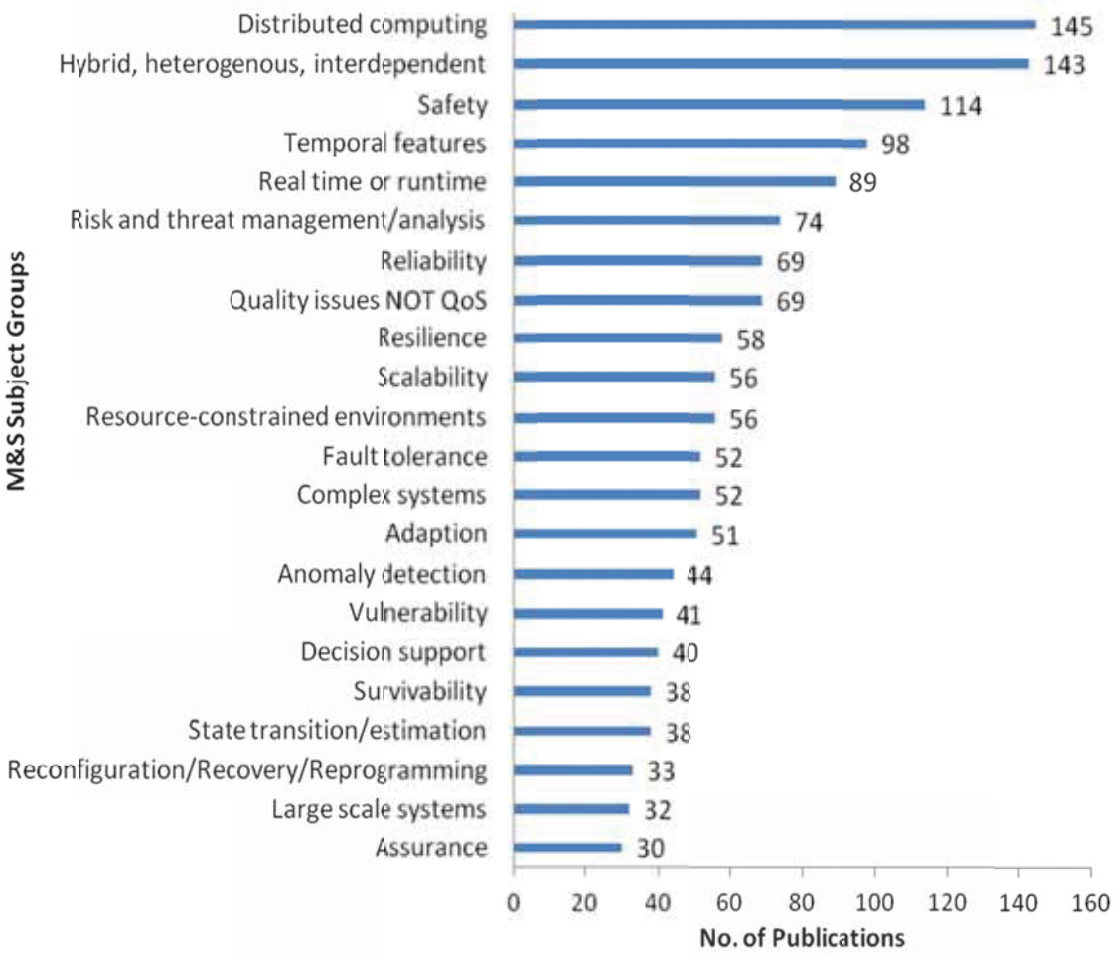


Figure 37. M&S Subset: Features or Attributes, ≥30 Publications, 2003-2013

Figure 38 documents publication trajectories for features with ascendant performance post 2008. In this view, even though absolute numbers are not great, one sees particular increases for topics such as *Real time or runtime, Data injection attacks*, and *Resilience. Real time or runtime*, for instance, increases from a single publication in 2003 to twenty-two articles in 2012.

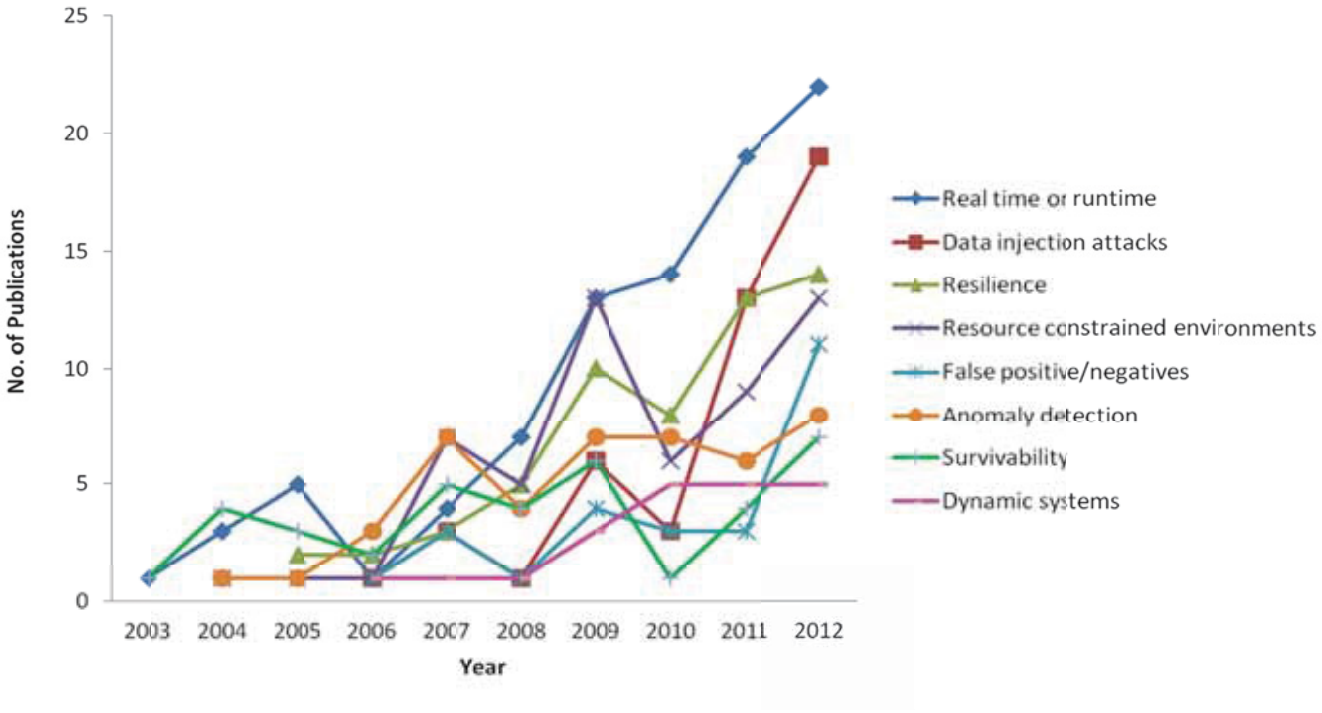


Figure 38. M&S Subset: Features or Attributes: Rising Numbers of Publications, 2003-2012

In the normalized view of performance (Figure 39), *Real time or runtime* and *Data injection attacks* remain at the top of the list, a testament to their enduring and growing research interest. *Reliability, Safety* and *Resilience* also feature prominently here. *Survivability*, while similar in nature, has a negative value relative to these topics. *Hybrid, heterogeneous, interdependent* and *Temporal features, which* ranked high in Figure 37 but had slightly declining numbers for 2011-2012, nonetheless also appear on the positive side of the distribution according to standard deviation.

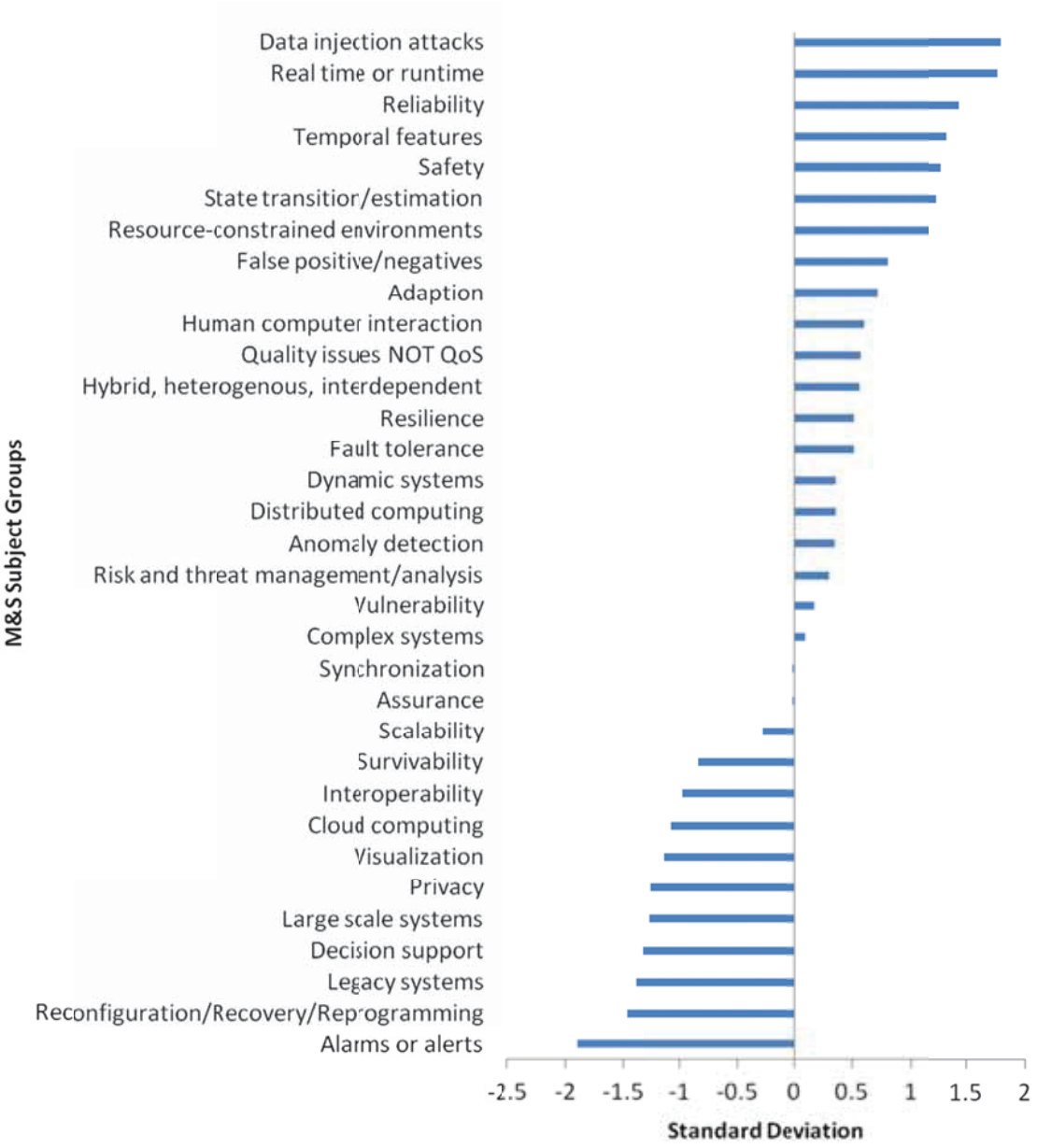


Figure 39. M&S Subset: Features or Attributes: Relative Rate of Research Interest, 2003-2012

4.2.3 Sectors or Application Areas

In Figure 40, we see publication counts for the top subject groups which describe *Sectors or Application Areas*. Sensor networks, public utilities, control systems and military applications all demonstrate strong performance in terms of numbers of publications.

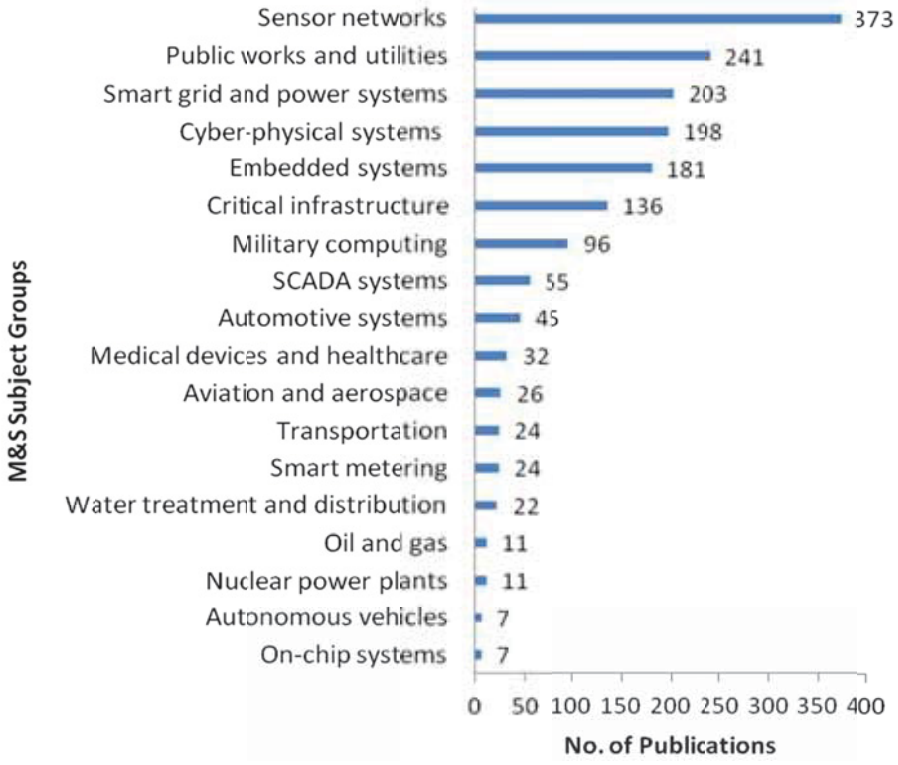


Figure 40. M&S Subset: Sectors or Application Areas, No. of Publications, 2003-2013

Post 2009, only six subject groups demonstrate an upward trend for publication counts. Two that show particular strength, *Cyber-physical systems* and *Embedded systems*, are quite generic in nature. This may indicate that, apart from the strong performance exhibited by electrical systems as seen in topical correlation maps and overall publication counts, most of the discussion of CPS cybersecurity still addresses the topic in general terms. Figure 41 does show an increase in publications for certain specific applications, such as automotive systems, but the numbers are slight, even at their 2012 peak.

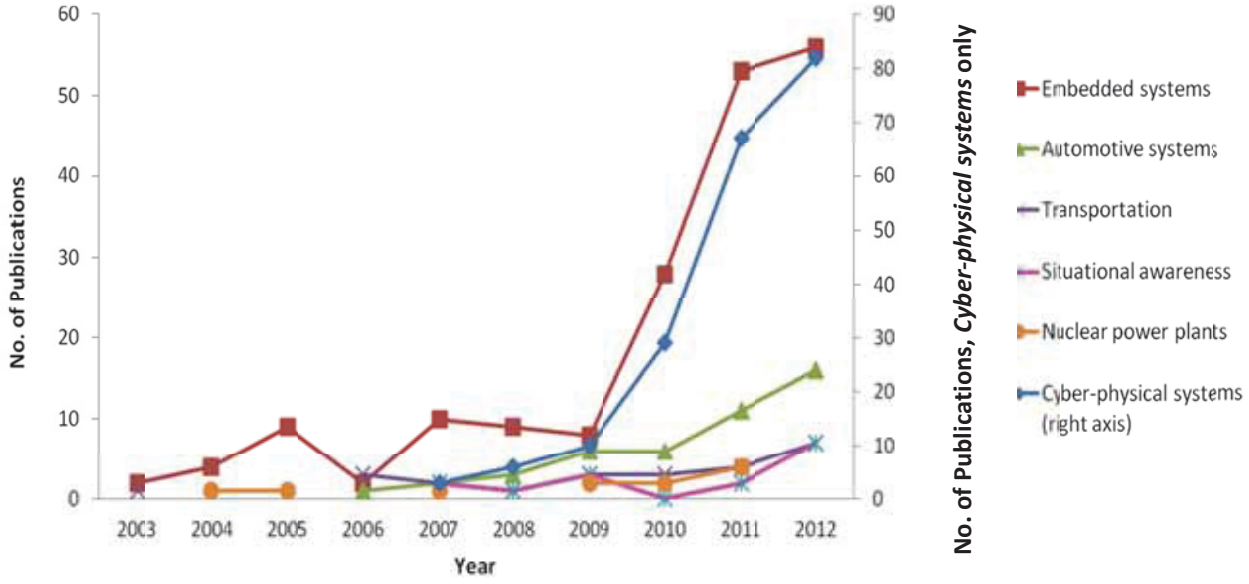


Figure 41. M&S Subset: Sectors or Application Areas, Rising No. of Publications, 2003-2012

In Figure 42, which shows the relative rate of research interest for subjects in this category, items with positive values also tend to be quite generic in nature, with a few exceptions (smart grid and metering, control systems, automotive systems), whereas those with negative values reference much more specific applications.

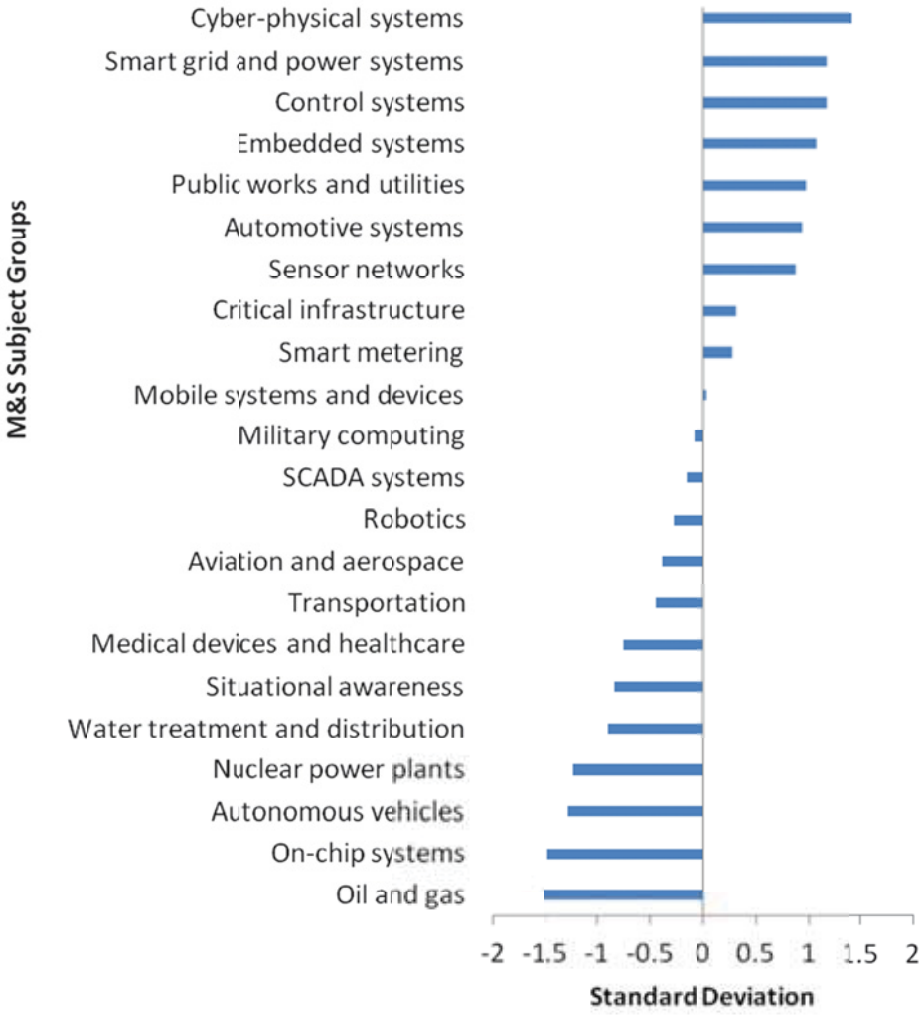


Figure 42. M&S Subset: Features or Attributes: Relative Rate of Research Interest, 2003-2012

4.2.4 Resilience

A key subject of interest for this project is the relationship between modeling or simulation and resilience in its various guises (survivability, recovery, adaptation, and so on). With regard to cyber-physical or embedded systems, DRDC wishes to review what is being modeled, and why, and wishes to better understand how this relates to survivability as well as basic intrusion detection.

A precise answer to these questions can only be had by delving deeply into the actual articles collected by our survey. The literature suggests that the challenges are many. In one example of particular interest, published in 2012, a team of researchers noted the following:

> There have been many efforts to ensure the security of CPSs. These are primarily based on extending mechanisms that are already used to protect the separate (cyber and physical) components of CPSs. However, there is no formal security model for CPSs that addresses security in a unified framework, and that deals with security threats, hardware threats, network threats and physical threats, possibly combined…Traditional threat models are restrictive and do not adequately capture the security of CPSs. In particular, they typically exclude survivability and recovery. [17]

In this case, the researchers used game theory to develop a threat model which captured systems features as well as adversarial intent; their framework also addressed combined and dependent vector attacks and synchronization issues which are typical of CPS environments.

Whatever the current inadequacies of solutions may be, an exploration of the M&S subset via cluster graphs demonstrates that modeling[f] is indeed being explored as a means of predicting and assuring resilience or survivability in the cyber-physical domain. Modeling is also closely related to risk/safety, and risk reduction based on model-driven analyses of vulnerability to threats. Modeling and simulation are also being used to design software and hardware control systems for CPS.

For each of the cluster graphs which appear below, selected nodes are used illustrate co-occurrence between M&S and resilience concepts. References are provided for representative articles captured in the overlapping nodes. The Intellixir database provided for DRDC use can offer more complete, in-depth reading opportunities by drilling down on overlapping nodes.

[f] In the analyses which follow, the subject group *Models and modeling* was used as a proxy for both *Models and modeling* and *Simulation*, since these two groups overlap almost completely.

Figure 43 demonstrates that most articles in the M&S database which reference resilience concepts do so in the context of modeling. [22-25]

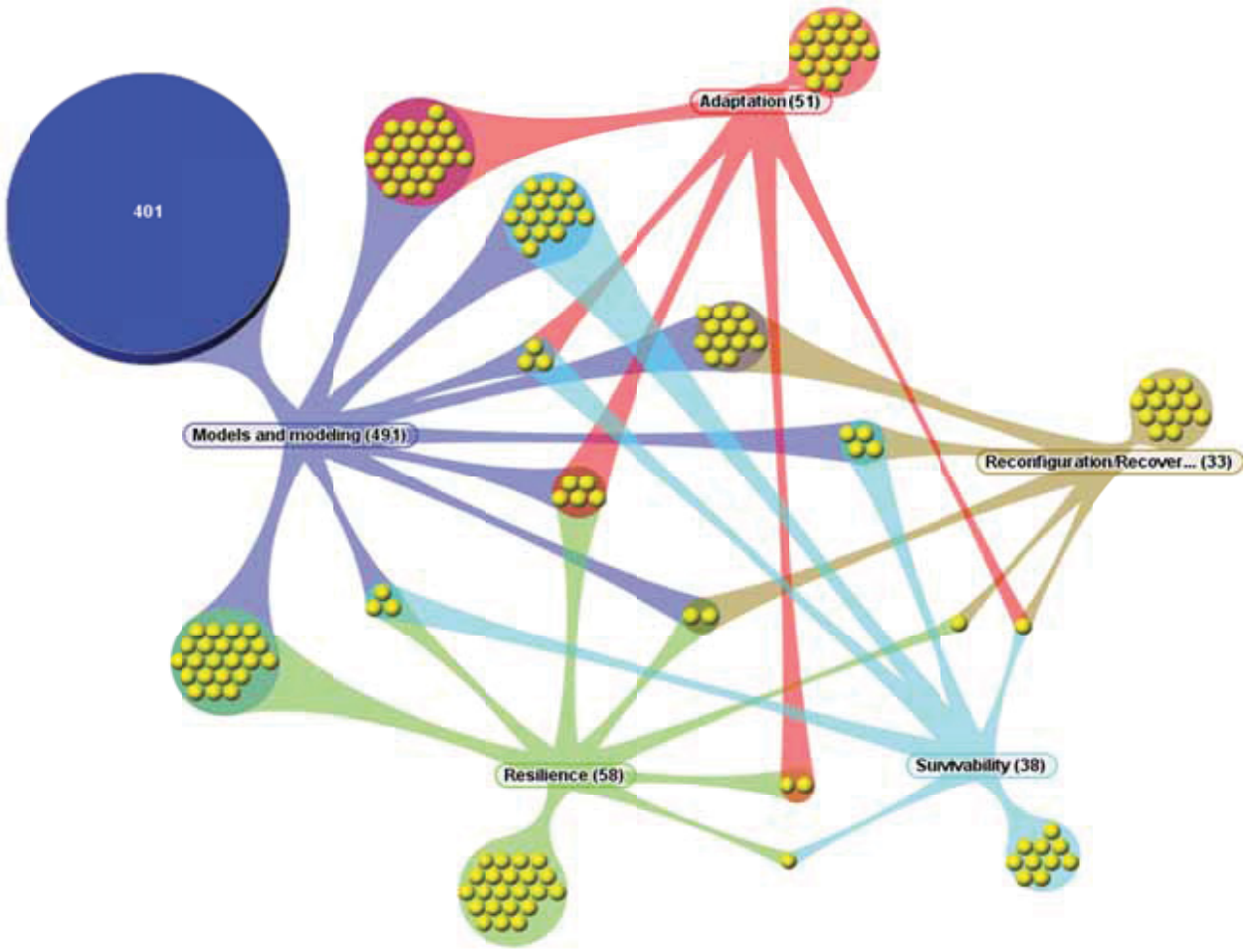


Figure 43. M&S Subset: Cluster Graph for Models and Modeling and Resilience Concepts

Safety and risk management are also discussed primarily as applications for modeling; resilience forms a key part of these assessments. [26-29]

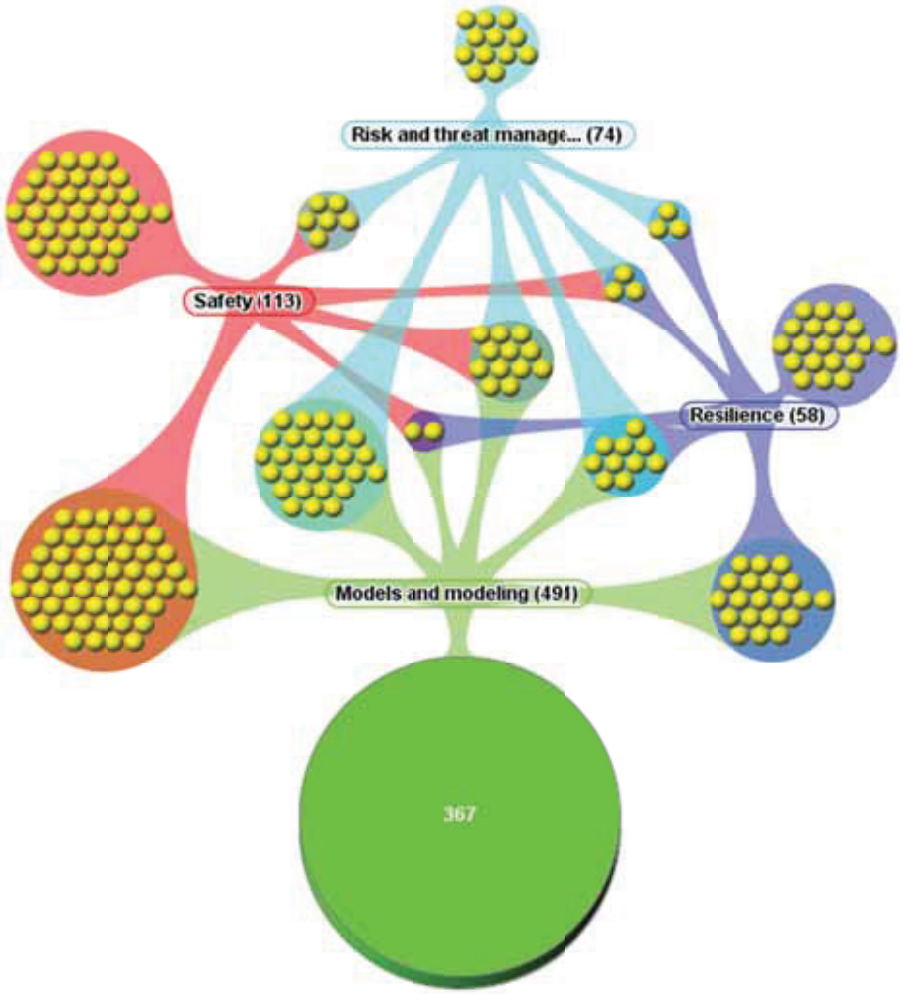


Figure 44. M&S Subset: Cluster Graph for *Models and Modeling, Safety, Resilience*, and *Risk*

There is also substantial exploration in the literature of how models may be used to improve the design and operation of software and controls in threatened environments. [30-36]

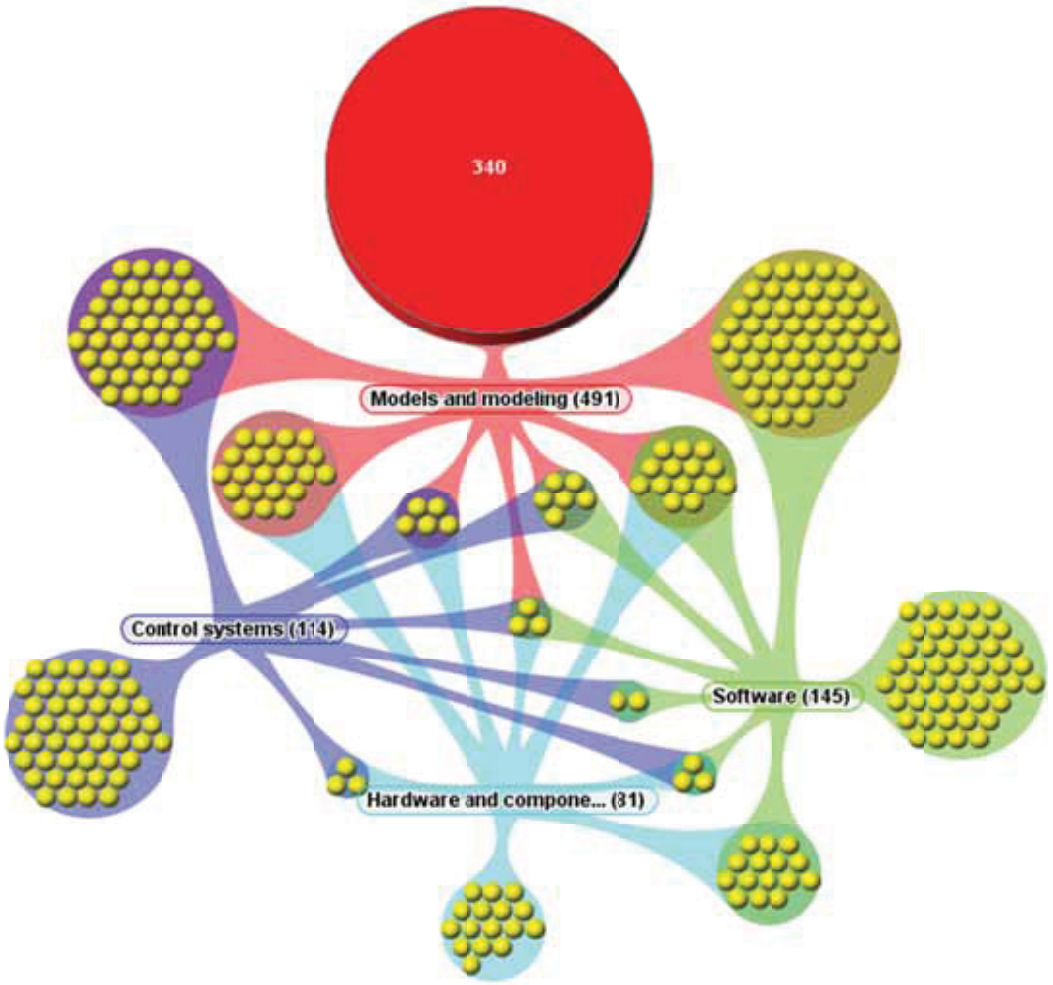


Figure 45. M&S Subset: Cluster Graph for Models and modeling, Software, Hardware, Control Systems

The subset also discusses how models can address real-time conditions in complex, hybrid, CPS systems. [37-41]

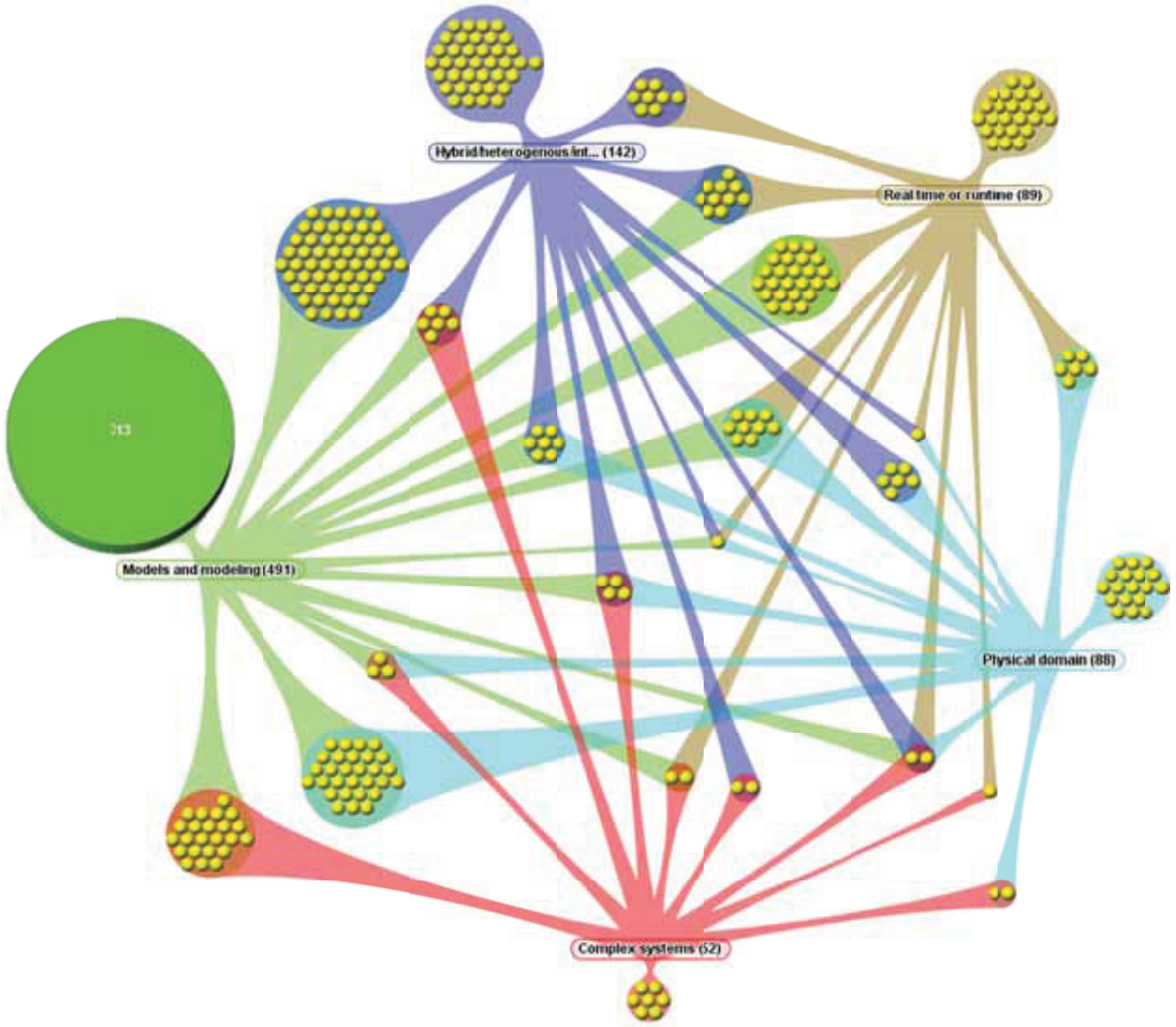


Figure 46. M&S Subset: Cluster Graph for Models and modeling, Real time, Hybrid and Complex Systems

In summary, the articles in the database on the topic of modeling and resilience make the following points:

- M&S techniques can be used to build threat/defence models, used to assess risk, vulnerability or survivability.[24]
- M&S must consider physical as well as cyber characteristics in an integrated fashion; techniques such as semantic agents may help extract and manage both types of characteristics.[42,43]
- Resilience should be built into system design (software, controls, system of systems); M&S can assist at all stages, from engineering through operations.[44,45]
- Cross-layer models can be used to manage security and reason about dependability needs and evolving states. Middleware and semantic methods may be used to manage communication between the layers.[46-48]
- Several recent articles also propose co-simulation platforms as a means of capturing cyber/physical complexity and mimicking their synergies.[49,50]
- There is a trade-off between robustness and resilience in most CPS systems; models should help optimize these.[51,52]
- CPS models should consider state awareness and uncertainty (e.g., via stochastic or behavioural modeling).[53-55]
- Probabilistic models and intelligent algorithms aid prediction. [29,56]
- Real time evaluation still presents a challenge.[37,57-59]

4.2.5 M&S Subset: Summary of Emergent Topics

In the M&S subset, the application of modeling and simulation to software design and security solutions is being actively discussed, although most papers are still exploratory in nature. This corpus of literature also appears to be gradually shifting focus from traditional network-based cybersecurity to research that integrates both the cyber and physical nature of critical infrastructures, embedded/SCADA systems, and industrial controls.

Overall, when both actual and normalized numbers are considered, one sees particularly strong performance over the last decade for large, generic subject groups such as *Models and modeling, Embedded systems,* and *Cyber-physical systems*. Excepting smart grids and wirelss sensor networks, there is rather less discussion of specific system types; however industrial controls, automotive and transportation applications have seen considerable research interest.

The dataset also stresses the criticality of *Safety, Reliability*, and *Resilience* and proposes model-based methods of risk assessment as a means of predicting threats and preventing system collapse.

The complexity of CPS systems and modeling is evidenced through rising interest in topics such as *Hybrid, heterogenous, interdependent* models, *Hierarchical frameworks*, *Real time and Dynamic systems.* Subjects such as *Middleware* and *Artificial intelligence/Learning* also demonstrate strong research iterest, presumably as they offer a technical means of addressing dynamic, many-layered CPS systems.

4.3 Major Players

4.3.1 Geographic Distribution

An analysis of geographic distribution of the affiliations associated with articles in the M&S subset (field coverage of 85% of the database) shows research strength in:

- United States (407 items, 40.5% of the dataset, a slight increase over the Master dataset)
- China (201 articles or 20%, an increase from 15.1% in the Master data)
- South Korea and India follow at some distance behind, with 33 publications each (3.3%)
- Germany records 31 titles (3%), Australia 28 (2.7%)
- Canada reports only 23 articles (2.3%)

Once again, these publication numbers include international co-publications.

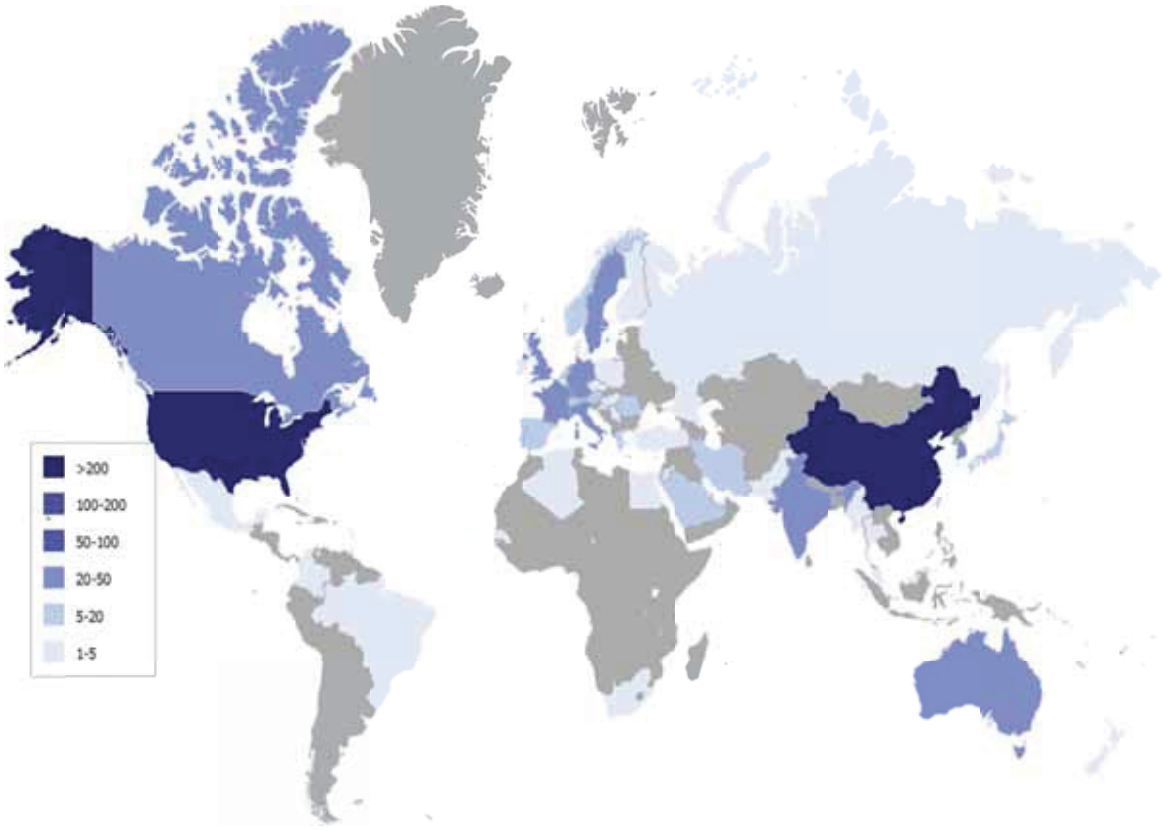


Figure 47. M&S Subset: Geographic Distribution of Publications, 2003-2013

4.3.2 Top Organizations

The top affiliations for the M&S subset appear in Figure 47. Once again, U.S. based academic institutions dominate, although the list is slightly more international in nature for M&S than was the case for the Master dataset.

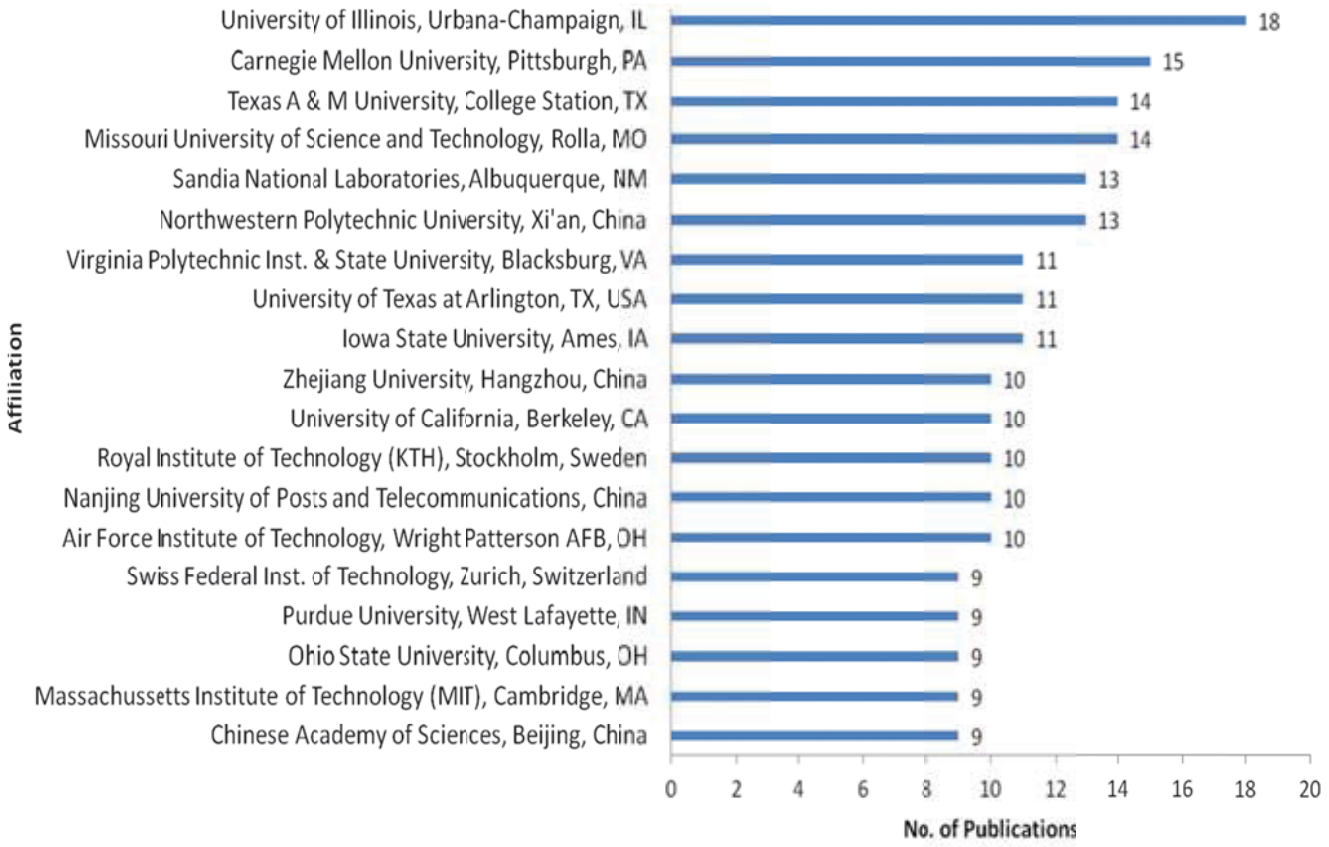


Figure 47: M&S Subset: Top Affiliations, ≥9 Publications, 2003-2013

4.3.3 Organization Types

Classification by type of affiliation (Figure 49) once again demonstrates that academic institutions dominate. While commercial institutions also are considerable in number, their percentage of publications in the subset drops to 10.15% in the subset (down from 15% in the Master dataset). Co-publications between Academic/Commercial , Academic/RTOs, and Academic/Military are substantial (Figure 50).

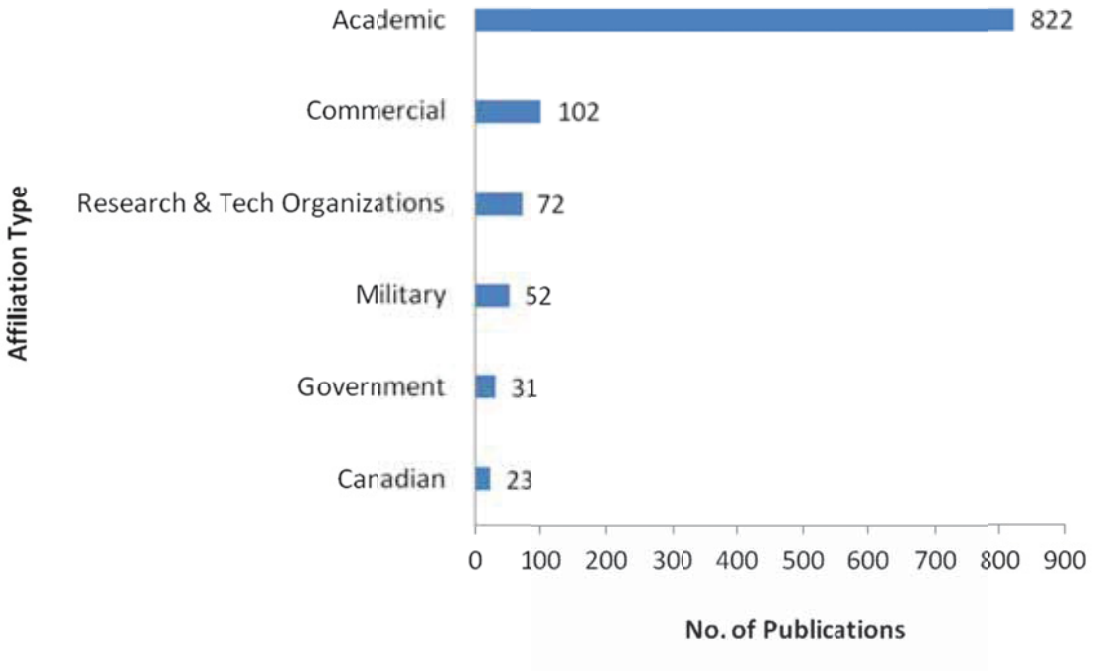


Figure 49. M&S Subset: Affiliations by Type, No. of Publications

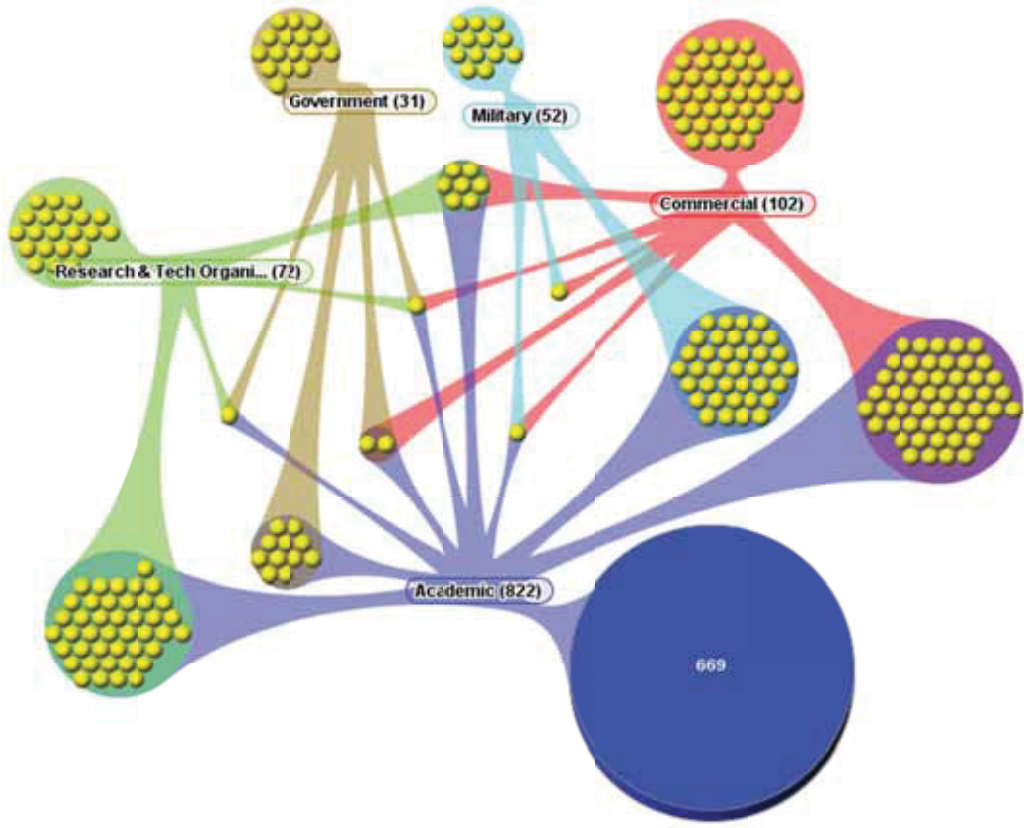


Figure 50. M&S Subset: Co-Publication by Type of Organization

In Table 8, the top organizations classified by category are listed.

Table 8. M&S Subset: Top Organizations by Category

Category	Top Organizations (# Publications)
Academic	• University of Illinois, Urbana-Champaign, IL, USA (18) • Carnegie Mellon University, Pittsburgh, PA, USA (15) • Missouri University of Science & Technology, Rolla, MO, USA (14) • Texas A&M University, College Station, TX, USA (14) • Northwestern Polytechnic University, Xi'an, China (13)
Government	• Sandia National Laboratories, Albuquerque, NM, USA (13) • Idaho National Laboratory, Idaho Falls, ID, USA (7) • Joint Research Centre, European Commission, Netherlands (3) • State Grid Electric Power Research Institute, Nanjing, China (2)
RTOs	• Royal Institute of Technology (KTH), Stockholm, Sweden (10) • Fraunhofer Inst. for Experimental Software Engineering, Kaiserslauten, Germany (6) • Electronics & Telecommunications Research Inst.(ETRI), Daejeon, South Korea (5) • Institute of Atomic Physics, Bucharest, Romania (3)
Commercial	• Electricité de France (EDF), Paris, France (5) • Associates in Communications Engineering Res.& Tech. (ACERT), Orlando, FL, USA (3) • Boeing Co., Sunnyvale, CA, USA (3) • CESI Ricerca, Milan, Italy (3) • MITRE Corp., McLean, VA, USA (3) • SRI International, Menlo Park, CA, USA (3)
Military[g]	• Air Force Institute of Technology, Wright Patterson AFB, OH, USA (10) • Air Force Research Laboratory, Rome, NY (8) • Air Force Research Laboratory, Wright Patterson AFB, OH, USA (6) • National University of Defense Technology, Changsha, China (5) • Naval Postgraduate School, Monterey, CA, USA (4) • Army Research Laboratory, Adelphi, MD, USA (3)
Canada	• University of New Brunswick, Fredericton, NB (4) • Concordia University, Montreal, QC (2) • DRDC CORA, Ottawa, ON (2) • McGill University, Montreal, QC (2) • Royal Military College, Kingston, ON (2) • U. British Coumbia, U. Calgary, U. Victoria, U. Ottawa (2 each)

[g] See Canadian category for contributions from DRDC CORA and Royal Military College. There is also one reference for DRDC Ottawa in the subset.

4.3.4 Co-Publication

Figure 51 shows instances of co-publication (two or more) between institutions with two or more publications in the M&S subset. As with the Master dataset (Figure 22), most instances of co-publication are between academic institutions, and same clusters in Ohio and New York state are apparent in the M&S subset (red nodes).

With the filter of ≥2 publications and ≥2 co-publications, one sees additional collaborations, particularly between academic institutions in China (turquoise nodes). Sweden's Royal Institute of Technology also assumes a central position in a lime green cluster linking academic organizations in Europe and India with commercial enterprises (Mecel AB, a systems and software company specializing in automotive applications, and Volvo).

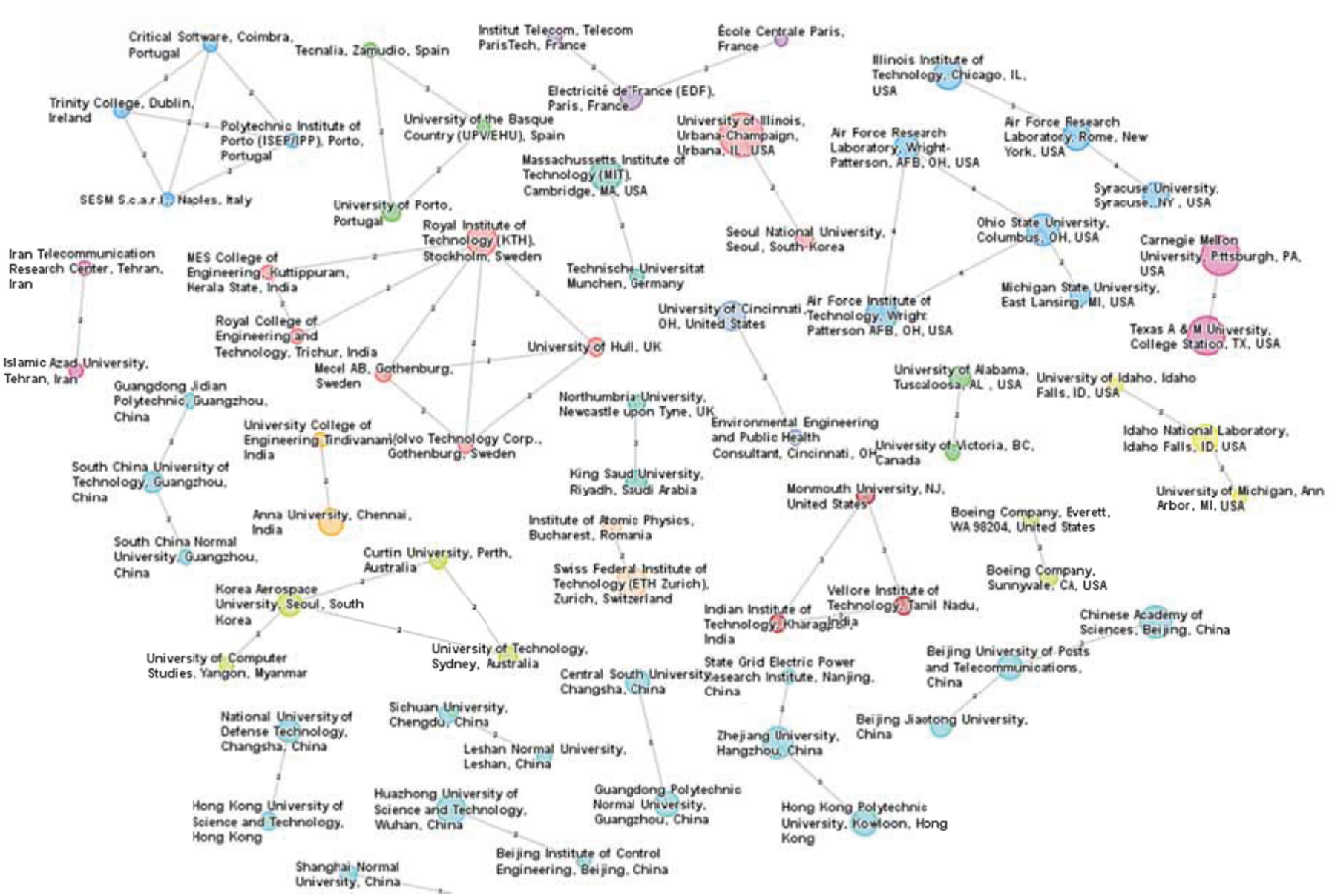


Figure 51. M&S Subset: ≥2 Co-Publications, ≥ Publications

Tables 9 and 10 provide further detail on organizational interests by presenting the top institutions and their publications strengths by subject group and heat-mapped to indicate the highest values in the table.

One sees particular expertise in American academic institutions and some Chinese organizations on modeling of wireless sensor networks, public works and the electrical grid. For non-academic institutions, U.S. based national laboratories and military organizations are also active in these same areas.

Of potential special interest to DRDC, given its interest in survivability aspects, is an apparent strength of the U.S. Air Force Research Laboratory in Rome, NY, on modeling and survivability.[60,61]

Table 9: M&S Subset: Academic Affiliations, 9 or more publications: Top Subject Areas

Total records	Affiliation	Models and modeling	Sensor networks	Wireless telecommunications	Simulation	Public works and utilities	Intrusion detection	Smart grid and power systems	Cyber-physical systems	Embedded systems	Distributed computing	Software	Hybrid, heterogeneous, interdep.	Critical infrastructure	Network security	Network protocols	Algorithms	Control systems	Safety	Temporal features	Military computing	Real time or runtime	Physical domain	Agents	Optimization	SCADA systems
18	University of Illinois, Urbana-Champaign, IL	8	4	4	4	7	1	7	10	5	2	4	5	3	2	3	2	5	4	4	4	2	4	1	5	
14	Missouri Univ. of Science and Technology, Rolla, MO	8	5	2	4	6	1	4	12	6	2	4	3	2	1	1	1			1			5	4	1	
14	Texas A & M University, College Station, TX	8	5	4	6	8	1	8	9	3	4	1	4	1	2	2	1					3	2	1	1	
13	Carnegie Mellon University, Pittsburgh, PA	10	2		2	5		5	5	8	2	4	1	3		2		2	3	1		1	1		1	1
13	Northwestern Polytechnic University, Xi'an, China	8	7	6	4	1	1	1	4	4		4	2	2	3	6	1	1	2	3		1	1		1	
11	Iowa State University, Ames, IA	6	2	2	5	6	1	6	3	2		2		1		1	1	3	5	1	1	2				4
11	University of Texas at Arlington, TX	5	10	9	8		3		2		1		1		1	6	3			1					1	
11	Virginia Polytechnic Inst. 7 State Univ. Blacksburg, VA	6	8	6	3	4	6	4	5	3	2	1	2	2	2	1	1	1	2	3	3			2	2	1
10	Nanjing Univ. Posts & Telecommunications, China	6	8	8	4	2	5	2	1				1		2	1	2			1			1			
10	Royal Inst. of Technology (KTH), Stockholm, Sweden	7	3	3		2	2	2	2	4	2	1	3	1	3	1	2	1	4						2	2
10	University of California, Berkeley, CA	8		1	2	2		2	8	3	1	1	3	1			2	2	4		1	1	1			2
10	Zhejiang University, Hangzhou, China	4	9	7	6	2	1	2	3	1	1				1	1	3				1		2			
9	Chinese Academy of Sciences, Beijing, China	6	2	1	1		3		1	1	2	2	1		3			1	1			1	1			
9	Massachusetts Institute of Technology, Cambridge, MA	5			1	2	1	2	4	3	4		3	2		1	2	2	2	3	1	3			1	
9	Ohio State University, Columbus, OH	3	5	3	6	5	2	3	2	2	3			5	1	1	6	2	2	3	2	2	2	1	1	1
9	Purdue University, West Lafayette, IN	5	2	1	3	2		2	4	4	1	5	3	1	1			1	1	1	1	1	2	1	1	
9	Swiss Federal Inst. Technology, Zurich, Switzerland	6	2	2	4	4	1	2	1	1	2	1	3	4		2	1	3	2	1		1			1	2

Table 10: M&S Subset: Non-Academic Affiliations, 3 or More Publications: Top Subject Areas

Total Records	Affiliation	Models and modeling	Sensor networks	Wireless telecommunications	Communications	Simulation	Public works and utilities	Intrusion detection	Smart grid and power systems	Cyber-physical systems	Embedded systems	Distributed computing	Software	Hybrid, heterogeneous, interdep	Critical infrastructure	Control systems	Reliability	Trusted computing	Survivability
13	Sandia National Laboratories, Albuquerque, NM	7			4	7	7	1	5	1			2	3	3	6	6		
10	Air Force Institute of Technology, Wright Patterson AFB, OH	2	2	1	6	5	7	1	6		1	2			4	4	2	6	1
10	Royal Institute of Technology (KTH), Stockholm, Sweden	7	3	3	2		2	2	2	2	4	2	1	3	1	1	2	1	
8	Air Force Research Laboratory, Rome, NY	5	2			2		2		1		4			2		1		8
7	Idaho National Laboratory, Idaho Falls, ID	4	3	1	1	2	2		2	1	1	1		1	2	4		1	
6	Air Force Research Laboratory, Wright-Patterson, AFB, OH	1	2	1	4	4	4	1	3			2			3	1	2	4	
6	Fraunhofer Inst. Experimental Software Engineering, Kaiserslautern, Germany	6									5		5		2		4		
5	Electricité de France (EDF), Paris, France	3								1				1	1				
5	ETRI, Daejeon, South Korea	4	2	1	2	3				4	3	2	1	2		1	1		
5	National University of Defense Technology, Changsha, China	2	4	4	2	4		1		1		2		1					
4	Naval Postgraduate School, Monterey, CA, USA	3			1	3	1					1		2	3				
3	Assoc. in Communications Engineering Res. & Tech (ACERT), Orlando, FL	1	3	3	2	1		3				2	2					1	
3	Boeing Company, Sunnyvale, CA	3	2		1		3		3			2				2		2	
3	CESI RICERCA, Milano, Italy	1			3	1	3		3							2			
3	Institute of Atomic Physics, Bucharest, Romania	2				1	1		1					1	2				
3	Joint Research Centre, European Commission, Netherlands	1			1	2	2		2				1		1	2			
3	MITRE Corporation, McLean, VA	2				2													
3	SRI International, Menlo Park, CA	3								3	3	1	1		1		1		
3	U.S. Army Research Laboratory, Adelphi, MD	3	2	3	2			2		1	1			1		1	1	2	

4.3.5 Top Authors

Top authors (5 or more publications) reported in the M&S dataset, and a brief statement as to their research interests, are shown below. Where active websites could be determined for these authors, URLs are embedded on the author name.

Table 11. M&S Subset: Top Authors (≥5 Publications)

Author	Institution	Topics	# Articles
Das, S. K.	University of Texas, Arlington, TX, USA	Game and epidemic theory (spread dynamics) for security in WSNs	8
Kundur, D.	formerly Texas A&M University, now University of Toronto, ON, Canada	M&S paradigms for smart grid dynamics & controls (vulnerability analysis, models of coordinated switching attacks)	6
Wang, Yun	Formerly Southern Illinois University, Edwardsville, IL; currently Bradley University, Peoria, IL	M&S of intrusion detection in Gaussian distributed WSNs	5
Zhang, Yuchen	Northwestern Polytechnic University, Xi'an, China	Task models in CPS; DoS resistant reprogramming in WSNs	5
Park, Jong Su	Korea Aerospace University, Seoul, South Korea	Recovery models for WSNs and CPS	5
Agrawal, D. P.	University of Cincinnati, OH	Intrusion detection in distributed Gaussian WSN networks	5
Zourntos, Takis	formerly Texas A&M	co-published with D. Kundur, above	5

4.3.6 Top Cited Authors (Citations External to M&S Dataset)

72% of the articles in the M&S subset include data for citations to previously published articles. Many of the top-cited authors in the subset also appeared as top-cited in the Master dataset. New to the M&S citation analysis in Table 12 are Estrin (UCLA) and Lee (Georgia Tech).

As for Table 6, which documented top cited references in the Master set, the subject areas of these authors may not be directly on point. The column on the far right of the table indicates the representation, if any, of these same authors in the M&S subset. Hyperlinks are provided where active websites were identified.

Table 12. M&S Subset: Top Cited Authors

Author	Affiliation	Research interests	# articles in M&S dataset citing this author	#articles by this author in M&S dataset
Perrig, A.	Carnegie Mellon University, Pittsburgh, PA (director of CyLab) and formerly ETH Zürich, Switzerland	Network and systems security for mobile computing and sensor networks	122	2
Stankovic, J.	University of Virginia, Charlottesville, VA	Real-time computing, cyber-physical systems, wireless sensor networks, and wireless energy and health applications.	98	2
Zhang, Y.	Microsoft Research, Beijing Labs; formerly HRL Labs of Malibu, CA and various U.S. academic institutions	Intrusion detection in WSNs; mobile and satellite networks	90	11
Wagner, D.	University of California, Berkeley, CA	Computer security, especially of large-scale systems and networks; smartphone and wireless security; applied cryptography	81	0
Culler, D.E.	University of California, Berkeley, CA	Network architectures for energy reduction, wireless embedded systems, parallel computing	79	0
Liu, Y.	University of South Florida, Tampa, FL; formerly a Ph.D. student at North Carolina State University, Raleigh, NC (under P. Ning, below)	Cybersecurity of wireless and CPS, especially smart grid	67	7

Author	Affiliation	Research interests	# articles in M&S dataset citing this author	#articles by this author in M&S dataset
Estrin, D.	University of California, Los Angeles , CA,	Embedded networked sensing systems, environmental monitoring applications, security of WSNs. "Most recently her work focuses on participatory sensing systems, leveraging the location, activity, image, and user-contributed data streams increasingly available from mobile phones."	63	0
Akyildiz, I. F	Georgia Institute of Technology, Atlanta, GA	Wireless networking; modeling, analysis and control of complex multi-scale data networks	57	1
Karlof, C.	Formerly University of California, Berkeley, CA (Ph.D. student), now a private security architect and software engineer	Full stack software development, mobile security and privacy	56	0
Lee, W.	Georgia Institute of Technology, Atlanta, GA; director of Georgia Tech Information Security Center; formerly North Carolina State University	Systems and network security, applied cryptography, network management, and data mining	51	0
Ning, P.	North Carolina State University, Raleigh, NC – currently on sabbatical with Samsung Mobile	Cloud computing security, wireless security, post-detection analysis of intrusion alerts	51	6
Su, W.	Naval Postgraduate School, Monterey, CA; former student of Ian Akyildiz (Georgia Tech), above	Sensor, satellite, and distributed networks; QoS; cybersecurity	49	0

5 SOURCES TO MONITOR

While not specified in the mandate, a request which emerged as part of ongoing project consultations concerned the top conferences and journals which may be of continuing interest. In Tables 13 and 14, the top sources are ranked according to the number of publications in the Master dataset. These same sources were mirrored in the M&S subset. Hyperlinks to conference webpages are provided where available.

Table 13. Master Dataset: Top Conferences (≥10 Publications)

Conference	# Publications, 2003-2013
IEEE Power and Energy Society (PES) General Meeting	44
IEEE Military Communications Conference (MILCOM)	41
International Symposium on Resilient Control Systems (ISRCS)	31
IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	26
IEEE PES Innovative Smart Grid Technologies (ISGT)	20
ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)	16
IEEE International Conference on Distributed Computing Systems (ICDCS)	15
IEEE International Conference on Communications (ICC)	14
IEEE International Conference on Computer and Information Technology (CIT), IEEE International Conference on Embedded Software and Systems (ICESS) [proceedings published together]	12
IEEE INFOCOM	12
Hawaii International Conference on System Sciences (HICSS)	12
International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)	11
International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface Technology (NPIC and HMIT)	10
IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing (iThings/CPSCom) [now separate conferences]	10

Table 14. Master Dataset: Top Serials (≥8 Publications)

Journal	# Publications, 2003-2013
Lecture Notes in Computer Science	128
Communications in Computer and Information Science	32
ACM International Conference Proceedings Series	23
International Journal of Critical Infrastructures	21
International Journal of Critical Infrastructure Protection	20
IEEE Transactions on Smart Grid	17
IEEE Security and Privacy	13
Proceedings of the IEEE	11
IET Conference Publications	10
Lecture Notes in Electrical Engineering	9
Advanced Materials Research	9
Journal of Networks	8
International Journal of Distributed Sensor Networks	8

6 CONCLUSIONS

The goal of this project was to provide an overview of the state of the art of security solutions for cyber-physical systems and to better understand how modeling and simulation techniques may contribute to those solutions, particularly with regard to increased resilience.

The literature survey conducted for this project indicates that interest in the area of cybersecurity for critical systems is keen, and for the most part, it has grown over the last decade.

Network-related security strategies such as cryptography or network intrusion detection have been, and will likely continue to be, central to the research agenda, inasmuch as they protect the communications architectures that keep entire systems running. For many researchers in the domain, however, traditional security approaches are found to be wanting. Over the course of the decade under review, an increase in supplementary techniques that address the special needs of the CPS environment is evident. Of particular interest in this regard are sophisticated methods that address safety, continued system availability, resilience, and behavior/anomaly patterns specific to particular applications. Real time and intelligent, adaptive/learning responses are also required, and show evidence of increased research interest.

Modeling and simulation are being used to enhance security at various stages, from system engineering through operations. Threat and defence models are being used to test system designs and detect anomalies. M&S techniques are also seen to contribute to vulnerability or risk assessments. In the literature, researchers also investigate stochastic and/or Markovian models or other learning methods as a means of detecting compromised components and of predicting system performance or recovery.

Most of the research conducted in this domain is being performed in academic institutions, and large American universities are key players. Commercial organizations also feature in scientific and technical publications, both as collaborators with academia and as research labs in their own right.

Of the applications or sectors described in the literature survey, wireless sensor networks and public utilities – especially electrical grids – are frequent subjects for research. Automotive, robotic, and industrial control networks constitute smaller segments, but show rising research interest.

Rising rates of publication in this field and the high degree of academic involvement both suggest that this topic has not yet reached maturity, or even an early plateau of interest. Indeed, all of the analyses conducted for this project support the observation, made in recent review literature, that cybersecurity for CPS is “in its infancy”. Some key challenges remain, especially in areas such as system complexity and interdependence as well as real time environments.

Various military applications and solutions are discussed in the literature, but the bulk of research conducted to date has focussed on sensor networks, public utilities, industrial controls and critical infrastructure such as electrical power grids, nuclear plants, or water distribution/treatment systems. Many of tomorrow’s solutions may arise from environments where continued operation is deemed critical to success and public security, even when the industry is not are overtly military in nature. Research partnerships may thrive in all of these application areas. Collaborations with private industry or public utilities may also support the military research agenda in areas such as wireless sensor networks, autonomous vehicles, avionics or vetronics. For that reason, we recommend that DRDC continue to monitor developments both inside and external to the military domain and to maintain a broad perspective when considering developments in CPS security.

7 REFERENCES

1. Keating T. *Resilient Systems Literature Survey.* Ottawa: NRC-CISTI;2012.
2. Bateman D, Gheorghe L, Hess B, Ludwig M, Olivereau A. Challenges and current results of the TWISNet FP7 project. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).* 2012;7449:232-233.
3. Gilbert S, King V, Saia J, Young M. Resource-competitive analysis: A new perspective on attack-resistant distributed computing. *Proceedings of the 8th ACM SIGACT/SIGMOBILE International Workshop on Foundations of Mobile Computing, FOMC'12.* 2012:1-6.
4. Chen RC, Hsieh CF, Huang YF. A new method for intrusion detection on hierarchical wireless sensor networks. *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, ICUIMC'09.* 2009:238-245.
5. Wei D, Lu Y, Jafari M, Skare P, Rohde K. An integrated security system of protecting smart grid against cyber attacks. In: proceedings from Innovative Smart Grid Technologies Conference, ISGT 20102010.
6. Matz S. Public-private resilience: State vs. private conceptions of security risk management in Danish cyber-based critical infrastructures. *Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011.* 2011:135-141.
7. Dimitrovski AD, Li H, Zhang Z, Gong S. Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Transactions on Smart Grid.* 2013.
8. Bhanu JS, Sastry JKR, SubbaRao K. Attacking embedded systems through fault injection. *Proceedings 2011 2nd National Conference on Emerging Trends and Applications in Computer Science (NCETACS 2011).* 2011:5.
9. Adhikari U, Morris TH, Pan S. Cyber security recommendations for wide area monitoring, protection, and control systems. *IEEE Power and Energy Society (PES) General Meeting.* 2012.
10. LaMonica M. Cybersecurity risk high in industrial control systems. . *MIT Technology Review* 2013.
11. Goertzel K. Software survivability: Where safety and security converge. *Crosstalk: The Journal of Defense Software Engineering.* 2009.
12. Larkin RD. *Evaluation of Traditional Security Solutions in the SCADA Environment [Masters' thesis]*. Wright Patterson AFB, OH: Air Force Institute of Technology; 2012.
13. Farooqi A, Khan F, Lee S, Wang J. A novel intrusion detection framework for wireless sensor networks. *Personal and Ubiquitous Computing.* 2012:1-13.
14. Barnum S, Sastry S, Stankovic J. Roundtable: reliability of embedded and cyber-physical systems. *IEEE Security & Privacy.* 2010;8(5):27-32.
15. Goertzel K. Survivable Software for Safety-Critical Cyber-Physical Systems. OWASP Application Security Conference (OWASP AppSec); 2012; Washington, DC.
16. Rieger C. Resilient control systems: Next generation design research. 2nd Conference on Human Systems Interactions; 2009.
17. Burmester M, Kagkos E, Chrissikopoulus V. Modeling security in cyber-physical systems. *International Journal of Critical Infrastructure Protection.* 2012;5:118-126.
18. Jha N, Raghunathan A, Aaraj N. A framework for defending embedded systems against software attacks. *ACM Transactions on Embedded Computing Systems (TECS)* 2011;10(3).
19. Li F, Wang X, Ning P, et al. A resilient real-time system design for a secure and reconfigurable power grid. *IEEE Transactions on Smart Grid.* 2011;2(4):770-781.
20. Sastry S. Networked embedded systems : From sensor webs to cyber-physical systems. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).* 2007;4416.
21. Simonite T. Old-fashioned control systems make U.S. power grids, water plants a hacking target. *MIT Technology Review.* 2012. http://www.technologyreview.com/news/429611/old-fashioned-control-systems-make-us-power-grids-water-plants-a-hacking-target/ Accessed February 10, 2013.

22. Martins E, deSousa F. A model-based approach for robustness test generation. In: proceedings from 5th Latin-American Symposium on Dependable Computing Workshops. 2011.
23. Filippini R, Silva A. A modelling language for the resilience assessment of networked systems of systems 2011; Available at: http://oa.upm.es/13033/2/INVE_MEM_2011_108973.pdf Accessed February 10, 2013.
24. Dixon C. Assessing vulnerabilities in interdependent infrastructures using attacker-defender models [Masters' thesis] 2011; Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a552169.pdf. Accessed February 10, 2013.
25. Bullo F, Pasqualetti F, Doerfler F. Attack Detection and Identification in Cyber-Physical Systems -- Part I: Models and Fundamental Limitations Accessed at 2012; Available at: http://arxiv.org/abs/1202.6144 Accessed February 10, 2013.
26. Crowther K. Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input-output model. *International Journal of Critical Infrastructure Protection.* 2008;1:53-67.
27. Babick J. *Tri-level Optimization of Critical Infrastructure Resilience [thesis]*. Monterey, CA: Naval Postgraduate School; 2009.
28. Alves-Foss J, Krings A, Oman P, de Leon D. Analyzing the security and survivability of real-time control systems. In: proceedings from Proceedings from the Fifth Annual IEEE System, Man and Cybernetics Information Assurance Workshop. 2004.
29. Queiroz C, Mahmood A, Tari Z, Goscinski A, Malhotra M. A probabilistic model to predict the survivability of SCADA systems. *IEEE Transactions on Industrial Informatics.* 2013:99.
30. Karsai G, Sztipanovits J. Model-integrated development of cyber-physical systems. . In: proceedings from Software Technologies for Embedded and Ubiquitous Systems. Proceedings 6th IFIP WG 10.2 International Workshop, SEUS2008.
31. Schneider D, Foerster M. Flexible, any-time fault tree analysis with component logic models. . In: proceedings from: IEEE 21st International Symposium on Software Reliability Engineering2010.
32. Becker M, DiPasquale A, Elfeky A, Mueller W. Virtual prototyping of cyber-physical systems. In: proceedings from 17th Asia and South Pacific Design Automation Conference (ASP-DAC)2012.
33. Cagabal G, Jung S, Kim S, Song J. Software vulnerability design and approaches for securing SCADA control systems. *International Journal of Smart Home.* 2009;3(1):49-56.
34. Xiaoyuan H, Yi X, Zhi T, Si G. Simulation Model of Cascading Effects from Cyber Attacks on Electric Power Infrastructure Networks. First International Conference on Instrumentation, Measurement, Computer, Communication and Control; 2011.
35. Ulieru M. Design for resilience of networked critical infrastructures. In: proceedings from Proceedings of the 2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference (DEST)2007.
36. Ambrosio R, Pournaras E, Yao M. Dynamic composition and reconfiguration of Internet-scale control systems. In: proceedings from IEEE International Conference on Digital Ecosystems and Technologies2011.
37. JC E, Lee E, Matic S, Seshia S, Zou J. Time-centric models for designing embedded cyber-physical systems. *UCB/EECS Technical Report.* 2009;2009-135:1-26. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-135.pdf.
38. Haslum K, Knapskog S, Moe M. Real-time intrusion prevention and security analysis of networks using HMMs In: proceedings from 33rd IEEE Conference on Local Computer Networks. 2008.
39. Wang Z. A hybrid model of rough sets and relevance vector machine for intrusion detection of internet of things. *Journal of Computational Information Systems* 2012;8(23):9881-9886. http://www.jofcis.com/publishedpapers/2012_8_23_9881_9886.pdf.
40. Sedigh A, Lin J, Hurson A. An agent-based approach to reconciling data heterogeneity in cyber-physical systems. In: proceedings from IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA)2011.

41. Jing L. An Agent-Based Approach to Reconciling Data Heterogeneity in Cyber-Physical Systems In: proceedings from IEEE International Symposium on Parallel and Distributed Processing Workshops and PhD Forum.2011.
42. Gandi R, Mahoney W. An integrated framework for control system simulation and regulatory compliance monitoring. *International Journal of Critical Infrastructure Protection.* 2011;4(1):41-53.
43. Miller A, Sedigh S, Lin J. A semantic agent framework for cyber-physical systems. *Semantic Agent Systems.* Vol 344. : Publisher; 2011.189-213.
44. Navarre D, Palanque P, Barboni E. Designing for resilience to hardware failures in interactive systems: A model and simulation-based approach. *Reliability Engineering & System Safety.* 2011;96(1):38-52.
45. Barrett B, J C, Cutchner-Gershenfeld J, Leveson N, Dulac N. Engineering resilience into safety-critical systems. *Resilience Engineering: Concepts and Precepts* 2006. http://sunnyday.mit.edu/papers/resilience-chapter.pdf.
46. Denker G, Dutt N, Mehotra S. Resilient dependable cyber-physical systems: a middleware perspective. *Journal of Internet Services & Applications* 2011. http://www.ics.uci.edu/~dsm/cypress/paper/grit2011.pdf
47. Hefeida M, Khokhar A, Kshemkalyani A, Shen M. Cross-layer protocols for WSNs: a simple design and simulation paradigm. In: proceedings from International Wireless Communications and Mobile Computing Conference2012.
48. Kim H, Kim W, Kim J, Kim J. A study on design of communication protocol for CPS simulation. *Advanced Materials Research.* 2012;488-489:881.
49. Al-Hammouri A. A comprehensive co-simulation platform for cyber-physical systems. *Computer Communications.* 2012;36(1):8-19.
50. Liang D, Wang Y, Zhou X. Study on integrated modeling methods toward co-simulation of cyber-physical system. Proceedings of the 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems 2012.
51. Chan A, Haines J, Johnson A, Mayberry T, Okhravi H. Dedicated vs . distributed : A study of mission survivability metrics. Military Communications Conference (MILCOM) 2011.
52. Zhu Q, Basar T. Robust and resilient control design for cyber-physical systems with an application to power systems. . IEEE Conference on Decision and Control and European Control Conference; 2011.
53. Alves-Foss J, Linda O. Towards resilient critical infrastructures : application of Type-2 Fuzzy Logic in embedded network security cyber sensor. International Symposium on Resillient Control Systems (ISRCS); 2011.
54. Chen K, Song X, Wang Z, Zhu Y. Reliability modeling method for network system using generalized stochastic petri net. International Conference on Quality ; Reliability ; Risk ; Maintenance ; and Safety Engineering (ICQR2MSE); 2012.
55. Chang P, Fiondella L, Lin Y. Quantifying the impact of correlated failures on system reliability by a simulation approach. *Reliability Engineering & System Safety.* 2013;109:32-40.
56. Rrushi J. Anomaly detection via statistical learning in industrial communication networks *International Journal of Information and Computer Security.* 2011;4(4):295-315.
57. Zhang Y, Duan W, Wang F. Architecture and real-time characteristics analysis of the cyber-physical system. IEEE 3rd International Conference on Communication Software and Networks. ; 2011.
58. Liu X, Tan F, Bu L, Cao J, Li T, Wang Q. From offline toward real-time : A hybrid systems model checking and CPS co-design approach for Medical Device Plug-and-Play (MDPnP). ACM/IEEE International Conference on Cyber-Physical Systems; 2012.
59. Dyke S, Gao X, Gill C, Hunag H, Lu C, Tidwell T. Cyber-physical systems for real-time hybrid structural testing : A case study. ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS); 2010.
60. Kwiat K, Macalik M, Kun X, et al. A Workflow-Based Non-intrusive Approach for Enhancing the Survivability of Critical Infrastructures in Cyber Environment. In: proceedings from International Workshop on Software Engineering for Secure Systems (SES 2007). 2007.

61. Kwiat K, Park J, Kamhoua C. Surviving in cyberspace : A game theoretic approach. *Journal of Communications* 2012;7(6):436-450.

8 APPENDICES

8.1 Attachments

- *STI 14926: Appendix 1: Topical Correlation Maps [Word document with large scale graphics]*

8.2 Methodology

8.2.1 Searches

Searches for this report were conducted in various databases: Scopus (Physical Sciences), INSPEC, National Technical Information Service (NTIS), IEEE xPlore, ACM Digital Library, Defense Technical Information Center (DTIC), and the NATO Science and Technology Organization database. Internet searches were conducted for project literature and presentations from defence agencies such as the Defense Advanced Research Project Administration (DARPA) and in order to collect project literature and conference proceedings not indexed elsewhere. Finally, a client-supplied list of around 200 additional bibliographic references was enriched with keywords, affiliations, and abstracts and added to the database of results.

In the bibliographic databases, searches were delimited to substantive fields (AB/TI/KW) and terms were combined using both Boolean (AND/OR) and proximity (NEAR) operators. Truncation (*) was also used to gather variant forms of words.

From the table below, terms from columns A were combined with column B using AND. Column A terms were also searched in combination with either Column C OR D terms.

Table 15. Search Terms

A: Critical Systems	B: Cyber-Security or CyberThreats	C: Security-Related Resilience	D: Modeling & Simulation
• Cyber()physical systems • Embedded system* • Critical infrastructure* • Critical system* • Mission critical • SCADA or supervisory control and data acquisition • industrial control systems • industrial networks • vetronic* • In-vehicle network* • Automo* NEAR (network* or IT or electronic* or information technolog*) • Satellite systems • Navigation systems • Unmanned vehicles (UAVs , UGVs, UUVs) • Air traffic control* • Weapon* system* • Critical NEAR utilit* • Smart grid* or power grid* • Power system* • Nuclear NEAR (plant* OR system* OR facil*) • Gas pipeline* • Water w/2 (suppl* or treatment) • Machine to Machine (M2M) Networks • Medical device* • wireless sensor network* OR WSN • Internet of Things	• Cyber()security • Cyber()crime* • Cyber()attack* • Cyber()terror* • Cyber()safe* • Cyber()threat* • Cyber()architecture* • Hack* • Malware • (Computer or internet) w/1 (virus or worm*) • Bot or bots • Botnet* • Stuxnet • Ghostnet • Trojan horse* • Intrusion detection 1. Security or safety or attack* or threat*	• Resil* • Fault* near toleran* • Tolera* • Redund* • Survivab* • Self-adapt* or self-heal* or self-repair* or self-correct* or reconfigur*	• Model* • Simulat* • Rules • Algorithm* • Agent-based • Multi-agent* • Common types, e.g., Markov, BDMP, Monte Carlo, genetic, Bayesian, learning , evolutionary, Petri net*, attack tree*, threat tree*, stochastic* • (predict* or probab* or analy* or cluster* or classif* or state estimat*) NEAR (model* or simulat*) • Statistic* OR numeric* • Game theor*

After initial scoping and review of results, at the request of the client, approximately 300 articles were manually weeded to remove articles which referenced network or communications cybersecurity exclusively (i.e., those articles where the physical elements were absent or insubstantial).

The search period covered the last 10 years, inclusive (2003-2013).

After removal of duplicate titles, the final Master dataset of results numbered 2,220 articles. From these data, a subset was created by searching in the keyword, title or abstract fields for all instances of either *model* OR simulat**. The Modeling and Simulation subset numbers 1,004 articles.

8.2.2 Analysis

All references were downloaded into VantagePoint and Intellixir software for analysis. Both of these platforms enable the creation of various groupings, statistical analyses, matrices, graphs, and cross-correlations used in the analysis of subjects, timelines, and player activity. The methods used to compute values or extract terms may differ according to the software used, causing small differences for some views. Most cleaning and processing was conducted in VantagePoint, and the resultant data was exported to Intellixir, where various additional visualizations are available.

In VantagePoint, database fields for keywords, identifiers, descriptors, and subject headings were merged into one field to create a single point for subject analysis. To obtain 100% coverage, words and phrases were also extracted from the title field and merged with other subject terms into the comprehensive keyword field. Words and phrases in this field were then cleaned to normalize variant spellings and acronyms and to combine synonyms. The top 300 keyword terms, used for creation of cluster/co-occurrence maps, constituted 96% of database content.

Keywords were also organized into 117 subject groups, created according to high frequency patterns in the top terms, concepts noted in the mandate, and readings from recent review articles which suggested possible important or emergent topics (for example, stochastic or behavioural models). Categorization into these groups is non-exclusive: for instance, a heading on threat models for electrical power distribution might be classified under both *Smart grid* and *Models and modeling*. Records referenced in the 117 subject groups constituted 98% of database content.

Normalized Rates of Research Interest

To ascertain the normalized growth rates and compare values according to their standard deviation for each of the subject groups in the genre categories, we plotted publication rates and the angle (slope) of their increase or decline over time over time, using linear regression. Average slope degrees and standard deviation were then calculated and standardized, to produce Z-scores. These standardized scores can be used to reduce “noise” and identify topical areas with the greatest emergent growth rates (velocity) in the dataset, as well as the subjects showing sub-standard rates. One possible limitation may be absent publication values for certain years in a time series, so the analysis provided by z-scores should also be accompanied by a review of actual values over time.

Software: Analytical Tools

Different analytic al tools were used to generate graphs and other visualizations used in this report. While VantagePoint was the basis for bar and line graphs, Intellixir was used to create Aduna clusters, and collaboration maps. TouchGraph software was used for cluster analysis (visualization of correlations between subject terms or groups) and collaboration maps.

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

National Research Council Institute for Scientific and Technical Information
1200 Montreal Road, Building M-55
Ottawa, Ontario
Canada K1A 0R6

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Cybersecurity for Critical Systems : Literature Survey

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Brady, B.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
June 2013	108	61

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence Research and Development Canada – Valcartier
2459 Pie-XI Blvd North
Quebec (Quebec)
G3J 1X5 Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
15bu	SRE07-001-033

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
STI Assessment 14926	DRDC Valcartier CR 2013-188

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

To assist Defence Research and Development Canada as it develops cybersecurity strategies for cyber-physical systems (CPS), NRC Knowledge Management conducted a literature survey and analysis of 2,220 publications drawn from scientific and technical databases. The survey found that research attention is gradually shifting from conventional approaches to cybersecurity, such as intrusion detection, to those that include a more holistic and integrated view of both cyber and physical aspects. Modeling and simulation play a key role in developing and testing security systems. Various CPS-specific modeling methods, such as those that incorporate state estimation or intelligent , interactive layers are also being explored.

Because of the criticality of most cyber-physical systems and their role in national security, many CPS modeling solutions specifically address safety, reliability and risk management; resilience and survivability are key.

Key players in CPS cybersecurity are U.S. academic institutions and government laboratories, but commercial enterprise is also active. Much of the current research is being driven by security needs of wireless sensor networks and electrical grids, but other sectors, such as the automotive industry, are also participants. Because innovations may first be seen and research partnerships may thrive in domains that are not overtly military, it is recommended that DRDC maintain a broad perspective white pursuing its own research goals for CPS cybersecurity.

En vue de soutenir Recherche et développement pour la défense Canada (RDDC) dans l'élaboration d'une stratégie pour la sécurité des systèmes cyber-physiques (SCP), CNRC Gestion du savoir a effectué une analyse de 2220 notices bibliographiques extraites de la littérature scientifique et technique. L'étude a révélé que l'attention des chercheurs se déplace progressivement des approches traditionnelles de cybersécurité a une perspective plus holistique et intégrée des aspects cybers et physiques. La modélisation et la simulation jouent un rôle clé dans le développement et l'essai des systèmes de sécurité. Diverses méthodes de modélisation -spécifiques aux SCP sont à l'étude, y compris certaines intégrant l'estimation d'état, l'intelligence artificielle ou les couches interactives.

En raison de la nature essentielle de la plupart des systèmes cyber-physiques et de leur rôle dans la sécurité nationale, de nombreuses solutions de modélisation se penchent sur la sécurité, la fiabilité et la gestion des risques; la résilience et la survie sont considérées comme des qualités essentielles.

Les principaux joueurs du domaine de la sécurité des SCP sont des institutions universitaires et des laboratoires gouvernementaux américains, mais des entreprises commerciales sont également actives dans le secteur. Une grande partie de la recherche actuelle est motivée par les besoins de sécurité des réseaux de capteurs sans fil et des réseaux électriques, mais d'autres secteurs, comme l'industrie automobile, y participent également. Parce que les innovations peuvent d'abord être vues et des partenariats de recherche peuvent se développer dans des domaines qui ne sont pas ouvertement militaires, il est recommande a RDDC de maintenir une perspective large dans la poursuite de ses propres objectifs de recherche en matière de cybersécurité pour les systèmes cyber-physiques.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS

cybersecurity; cyber-physical systems; literature survey; risk management; wireless sensor network; survivability

Defence R&D Canada

Canada's Leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca