MEMS INERTIAL SENSORS FOR CYBER-PHYSICAL SYSTEMS: TRUSTWORTHY SENSING, S ECURE COMMUNICATION, DATA FUSION AND INFORMATION CONTROL

Liam Herlihy and Sergey Edward Lyshevski
Department of Electrical and Microelectronic Engineering
Rochester Institute of Technology
Rochester, NY 14623 USA
E-mail: Sergey.Lyshevski@mail.rit.edu URL: http://people.rit.edu/seleee

ABSTRACT

This paper examines inertial navigation systems (INS), robust information acquisition and secure communication with application for cyber-physical systems (CPS). These CPS comprise cyber and physical modules and subsystems. Advanced-technology networked sensor arrays enable distributed intelligence, as well as information acquiring, fusion, management and sharing by an *intelligent cloud*. *Cloud* level capabilities at the node level will enable key performance metrics of multi-level hierarchical distributed information management architectures. Our findings are demonstrated and substantiated by performing consistent technology evaluation and assessment in laboratory environment. Overall functionality, security, adaptiveness and situation awareness are improved.

Keywords: cyber-physical systems, data fusion, inertial sensors, security

1. INTRODUCTION

Our goal is to enable low- and high-level secure information acquiring, fusion and acquisition in systems with inertial sensors. Synergetic system-level integration of sensing technologies with processing paradigms is based upon consistent analyses and verification. This paper develops algorithmic and software solutions for advanced hardware (sensors, networks, interface and processors) within a hierarchical *cloud* architecture. By using proposed algorithms, protocols and tools, shared reconfigurable processing and on-demands sensor data fusion ensure superior performance and capabilities. The solutions are tested and evaluated in the laboratory environment. The software-hardware co-design at the *cloud* levels support adaptation and distributed intelligence to accomplish the following tasks: *Detect ↔ Process and Identify ↔ Assess, Manage and Control.*

Emerged sensing technologies [1-3] enable surveillance, target acquisition, reconnaissance, as well as decision and control. MEMS and solid-state technology sensor arrays enable processing at the node level in distributed environments. Hierarchical *cloud* architectures can be applied in various systems and platforms within adaptive information management schemes using secure communication, data fusion and distributed control. The proposed high-impact technology is based upon transformative solutions, practical hardware and substantiated software. The range of applications is very broad, e.g., from aerospace systems to transportation and healthcare. Our findings and solutions may contribute to control, intelligence, target acquisition, reconnaissance, surveillance and electronic warfare.

2. TECHNOLOGY DESCRIPTION

Our objectives are to initiate development of high-impact technology-centric solutions, empower engineering design at the system- and device- levels, as well as contribute to deployment of next generation of information management systems in various applications. To enable the existing technologies, we focus on:

- Data quality enhancement through adaptive processing, secure communication and *cloud* network security;
- Adaptive information management with shared processing resources and capabilities;
- Formative analysis and quantitative evaluation of distributed control, data acquiring and data fusion

Control, processing and information management tools for advance hardware must be developed using new hardware-specific software and algorithms. For inertial and navigation sensors in CPS, this paper:

1. Determines dependencies between sensor errors, accuracy and information losses;
2. Develops practical solutions to integrate networked distributed sensors in order to enable safety, security, functionality and information fusion, including detection of normalcy and abnormality;
3. Demonstrates and substantiates the findings reported.

With a focus on analysis of *cloud* CPS with INSs, one needs to procure MEMS/microelectronics technologies and hardware for data analytic, informatics and control. At the node level, one must: (i) Derive quantitative metrics between observable physical quantities and measurements; (ii) Assess information content of measured and processed data; (iii) Examine measurements and processed data using real data sets; (iv) Develop performance measures and metrics to assess data retrieval and fusion; (v) Examine and verify trustworthy sensing premises, security, as well as adaptive schemes and algorithms to improve data quality.

This paper researches *cloud* information acquisition and retrieval principles and architectures. A physics-consistent, technology-supported, information-centric multiple-level architecture is based upon cross-cutting technologies. The hardware under our studies is illustrated in Figure 1.

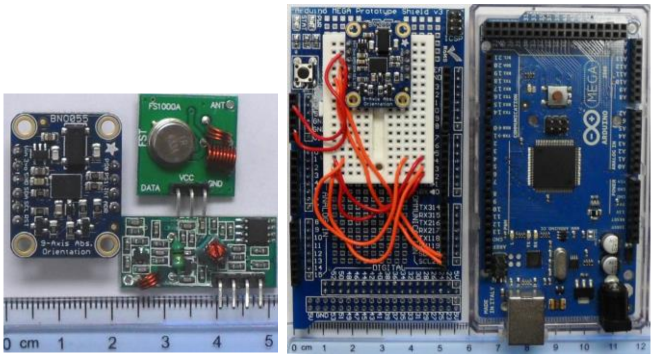

Figure 1. BNO055 INS, transmitter, receiver, and, Arduino MEGA 2560 board with BNO055

3. PROCESSING SOLUTIONS

3. 1. Processing and Acquisition Calculi

Enabled calculus and processing schemes are examined to achieve filtering, estimations and data fusion under uncertainties. Adaptive reconfigurable algorithms should enable physics-consistent data conformity [4-7]. The proposed processing scheme for the INS with an additional microcontroller (μC) is

$$\underset{\text{Acting Physical Quantities}}{\overset{\text{Acting Physical Stimuli}}{\mathbf{y}}} \Rightarrow \underset{\text{Measured Quantities}}{\overset{\text{Sensor Outputs}}{\bar{\mathbf{y}}}} \underset{\text{ASICs Processing}}{\overset{\text{Data Fusion}}{\Rightarrow}} \overset{\text{INS Outputs}}{\hat{\mathbf{y}}} \underset{\mu\text{C Processing}}{\overset{\text{Data Analytics}}{\Rightarrow}} \underset{\text{Transmitter}}{\overset{\text{INS-}\mu\text{C Outputs}}{\tilde{\mathbf{y}}}} \underset{\text{Secure Communication}}{\overset{\text{Data Transmission}}{\Rightarrow}} \underset{\text{Receiver}}{\overset{\text{Data Fusion INS-CPS}}{\hat{\mathbf{y}}}} . \quad (1)$$

The physical quantities $\mathbf{y}$ are acquired, measured, processed, transmitted and received with multispectral noise $\mathbf{n}$, error $\boldsymbol{\varepsilon}$ and distortions $\boldsymbol{\Delta}$. For all $\mathbf{y}_i$, one has $\mathbf{y}_i=\mathbf{y}+\mathbf{n}_i+\boldsymbol{\varepsilon}_i+\boldsymbol{\Delta}_i$. For example,

$\bar{\mathbf{y}}=\mathbf{y}+\mathbf{n}_{\bar{y}}+\boldsymbol{\varepsilon}_{\bar{y}}+\boldsymbol{\Delta}_{\bar{y}}$, $\hat{\mathbf{y}}=\mathbf{y}+\mathbf{n}_{\hat{y}}+\boldsymbol{\varepsilon}_{\hat{y}}+\boldsymbol{\Delta}_{\hat{y}}$ and $\tilde{\mathbf{y}}=\mathbf{y}+\mathbf{n}_{\tilde{y}}+\boldsymbol{\varepsilon}_{\tilde{y}}+\boldsymbol{\Delta}_{\tilde{y}}$.

Noise $\mathbf{n}$, error $\boldsymbol{\varepsilon}$ and distortions $\boldsymbol{\Delta}$ affect accuracy, precision, resolution, bandwidth and data fidelity. The observed $(\mathbf{n}_i,\boldsymbol{\varepsilon}_i,\boldsymbol{\Delta}_i)$ must be minimized. Using the concepts and algorithms reported in [6, 7], the IMU–μC outputs $\tilde{\mathbf{y}}=[(\tilde{a}_x,\tilde{a}_y,\tilde{a}_z),(\tilde{\omega}_\theta,\tilde{\omega}_\phi,\tilde{\omega}_\psi)]$ are found. The acceleration, velocity and position estimates are $\tilde{\mathbf{y}}_\Sigma=[(\tilde{\mathbf{a}},\tilde{\boldsymbol{\alpha}}),(\tilde{\mathbf{v}},\tilde{\boldsymbol{\omega}}),(\tilde{\mathbf{x}},\tilde{\mathbf{r}})]$. The representative experimental results for

$$\hat{\mathbf{y}}_\Sigma=\begin{cases}(\hat{a}_x,\hat{a}_y,\hat{a}_z),(\hat{\alpha}_\theta,\hat{\alpha}_\phi,\hat{\alpha}_\psi)\\(\hat{v}_x,\hat{v}_y,\hat{v}_z),(\hat{\omega}_\theta,\hat{\omega}_\phi,\hat{\omega}_\psi)\\(\hat{x},\hat{y},\hat{z}),(\hat{\theta},\hat{\phi},\hat{\psi})\end{cases} \text{ and } \tilde{\mathbf{y}}_\Sigma=\begin{cases}(\tilde{a}_x,\tilde{a}_y,\tilde{a}_z),(\tilde{\alpha}_\theta,\tilde{\alpha}_\phi,\tilde{\alpha}_\psi)\\(\tilde{v}_x,\tilde{v}_y,\tilde{v}_z),(\tilde{\omega}_\theta,\tilde{\omega}_\phi,\tilde{\omega}_\psi)\\(\tilde{x},\tilde{y},\tilde{z}),(\tilde{\theta},\tilde{\phi},\tilde{\psi})\end{cases}$$

are reported in Figures 2 and 3.

Derived outputs $\tilde{\mathbf{y}}$ ensure accuracy and precision in estimation of velocities, positions, orientation, trajectory, etc. The reported results significantly enable concepts reported in [1-3, 8, 9].

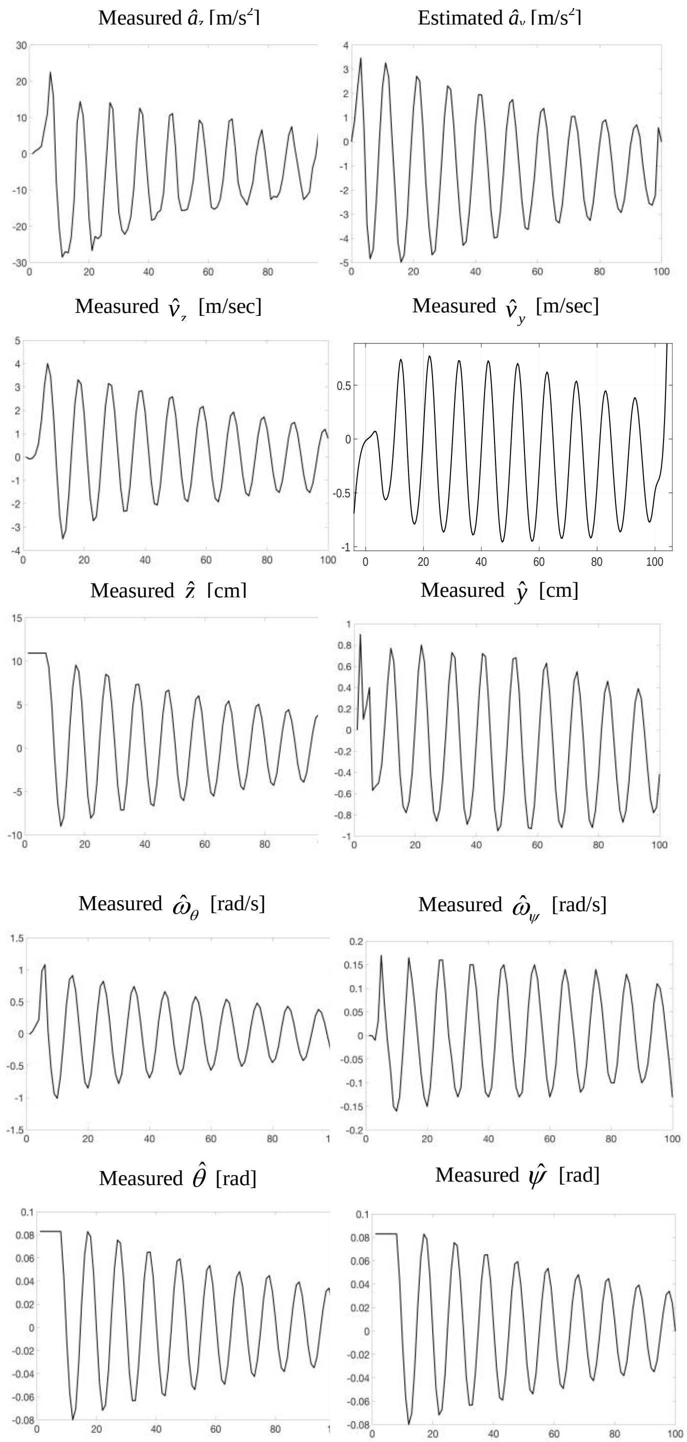

Figure 2. Measured asymmetric dynamics and bending motions of a beam. INS outputs: Linear accelerations, velocities and position for lateral $(\hat{a}_z,\hat{v}_z,\hat{z})$ and vertical $(\hat{a}_y,\hat{v}_y,\hat{y})$ motions, as well as angular velocities and displacements $(\hat{\omega}_\theta,\hat{\theta})$ and $(\hat{\omega}_\psi,\hat{\psi})$.

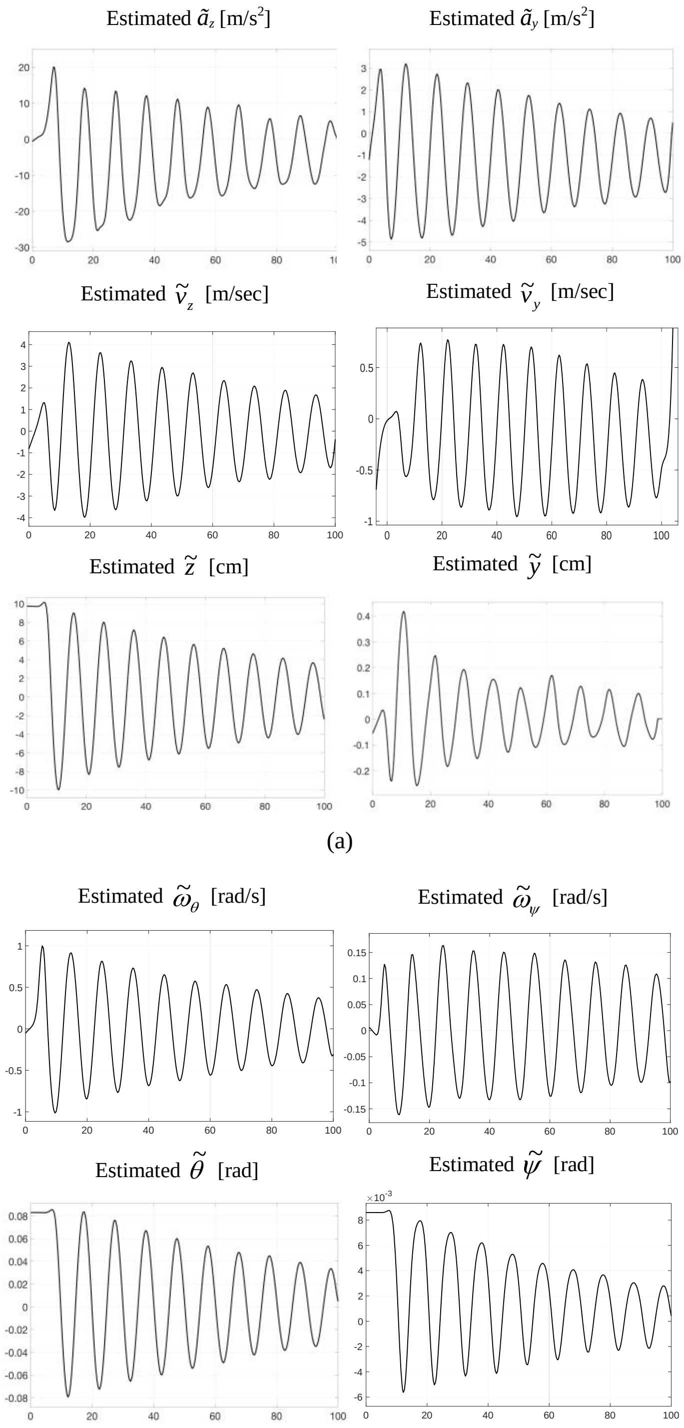

Figure 3. Asymmetric dynamics bending motions of a beam:
(a) Estimated linear accelerations, velocities and position for lateral and vertical motions $(\tilde{a}_z, \tilde{v}_z, \tilde{z})$ and $(\tilde{a}_y, \tilde{v}_y, \tilde{y})$ motions;
(b) Angular velocities and displacements $(\tilde{\omega}_\theta, \tilde{\theta})$ and $(\tilde{\omega}_\psi, \tilde{\psi})$.

Information Losses – For physical stimuli with accelerations $\mathbf{y}=[\mathbf{a},\boldsymbol{\alpha}]$, using the output vector $\hat{\mathbf{y}}$, the post-processed estimates $\tilde{\mathbf{y}}_\Sigma=[(\tilde{\mathbf{a}},\tilde{\boldsymbol{\alpha}}),(\tilde{\mathbf{v}},\tilde{\boldsymbol{\omega}}),(\tilde{\mathbf{x}},\tilde{\mathbf{r}})]$ are found. The physical $\mathbf{y}_\Sigma=[(\mathbf{a},\boldsymbol{\alpha}),(\mathbf{v},\boldsymbol{\omega}),(\mathbf{x},\mathbf{r})]$ can be measured using high-speed camera, high-accuracy sensors and other techniques to evaluate the accuracy, preciasion and information losses.

The estimates $\tilde{\mathbf{y}}_\Sigma$ are compared with the physical quantities $\mathbf{y}_\Sigma$. The information losses $\mathcal{D}$ and $\mathcal{D}_t$ are expressed as [7]

$$\mathcal{D}=\frac{1}{\|\mathbf{y}_\Sigma\|_p}\left\|\,|\mathbf{y}_\Sigma|-|\tilde{\mathbf{y}}_\Sigma|\,\right\|_p,\ \mathcal{D}_t=\int_T \frac{1}{\|\mathbf{y}_\Sigma\|_p}\left(|\mathbf{y}_\Sigma|-|\tilde{\mathbf{y}}_\Sigma|\right)dt, \qquad (2)$$

$\mathcal{D}\le\delta$, $\mathcal{D}_t\le\delta_t$, $\delta\ge0$, $\delta_t\ge0$.

If there are no information losses, $\mathcal{D}$=0 and $\mathcal{D}_t$=0.

To minimize errors and information loss, one should minimize $(|\mathbf{y}_\Sigma|-|\tilde{\mathbf{y}}_\Sigma|)$ by minimizing errors $\boldsymbol{\varepsilon}$, uncertainties and distortions $\boldsymbol{\Delta}$. The minimization problem $\min\limits_{\mathcal{D}(\boldsymbol{\varepsilon},\boldsymbol{\Delta})}\min\limits_{\mathcal{D}_t(\boldsymbol{\varepsilon},\boldsymbol{\Delta})}\left[\mathcal{D}(\boldsymbol{\varepsilon},\boldsymbol{\Delta}),\mathcal{D}_t(\boldsymbol{\varepsilon},\boldsymbol{\Delta})\right]$ may be solved using a principal component analysis [7].

Applications – The results are applied to solve control [5, 6, 10] and identification [11] problems. The inertial and navigation sensors are used to control complex electromechanical and mechanical systems [12-16]. To optimize physical systems, the displacements, velocities and accelerations are used as the state variables to implement control laws and design management systems.

4. SECURE COMMUNICATION

Secure wireless communication is studied. To overcome security vulnerabilities, we examine advanced encryption schemes with an emphasis on identity-based cryptography. Advanced Encryption Standard (AES) and authentication protocols are used. Using the permutation-substitution-permutation-network, the AES block cipher may ensure permutation of the SubBites, ShiftRows and MixColumns operations. With a key K on a message P, the encryption is expressed as $C=E_K(P)$ with the ciphermessage C. For decryption with a key K, $P=D_K(C)$. For symmetric encryption, $P=D_K(E_K(P))$. The full strength asymmetric AES-256 is considered.

The cryptanalysis is studied by analyzing the cryptosystem using an algebraic form $\mathbf{F}_{2^8}[z]$, and

$$S(b)=s_0\oplus\bigoplus_{i=1}^{8} s_i\odot b^{255-2^{i-1}}. \qquad (3)$$

Byte transformations, state shifting, column transformations and other operations are performed by transforming bites (SubBytes), shifting rows (ShiftRows) and mixing columns (MixColumns).

The AES-256 is implemented using an 8-bit, 16 MHz microcontroller. The full-strength keys are generated at each transmission. The encrypted messages are transmitted and decrypted. The timing for the encryption–decryption sequences are illustrated in Figure 4. The total latency is algorithm-specific and processor-dependent. For the experiments, it varies from 0.4 to 0.6 msec. A fragment of the key generation sequence is reported. The use of advanced microcontrollers drastically reduces the latency.

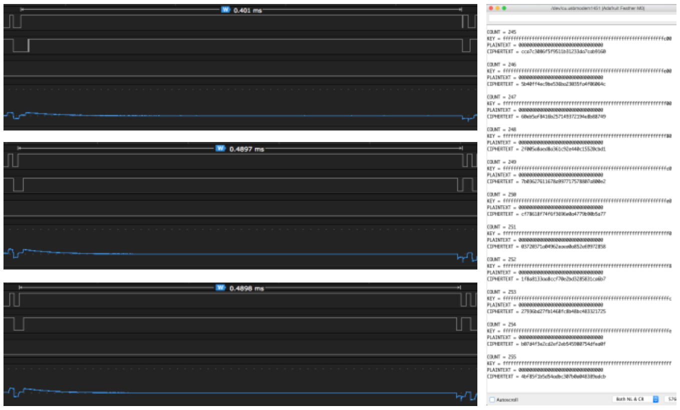

Figure 4. Encryption–decryption sequences, and, key generation sequence

5. CONCLUSIONS

The proposed intelligent and secure information acquisition, fusion, retrieval and management will enable situation assessment and situation awareness over different platforms and environments. New processing calculi and algorithms were developed and justified to enable accuracy and precision of inertial and navigation sensors. The reported high-impact technology ensures physics-based, processing-compliant and system-centric information management for heterogeneous data. The key advantages of our research and developments are:

1. Robustness and operation in adverse environments;
2. Modularity and scalability for large-scale CPS;
3. Redundancy, resilience and adaptiveness;
4. Information security, confidentiality and authenticity;
5. Information conformity, consistency, completeness and validity.

The aforementioned features guarantee overall functionality, enable capabilities and increase mission effectiveness.

Impact – The proposed solutions may be investigated for control and intelligence systems to enable risk-aware surveillance, target acquisition, reconnaissance, etc.

Architecture, Hardware Solutions and Technology Readiness Level – The technology-proven ASICs, FPGA, microcontrollers, MEMS/solid-state sensors, IMUs and INSs were studied. Analytical and laboratory studies to validate components of *cloud* architecture, methods, information management algorithms and information acquisition technology elements were carried out.

Technology Transfer – We performed and demonstrated basic, analytic and laboratory studies to validate methods, algorithms and technology elements. The proof-of-concept hardware and proven solutions enabled potential transfer of our findings to high-fidelity operational environment in various applications and diverse platforms.

REFERENCES

[1] G. Chatterjee, L. Latorre, F. Mailly, et. all., "MEMS based inertial measurement units for strategic applications", *Proc. Symp. Design Test Integration and Packaging of MEMS and MOEMS*, pp. 1-5, 2015.

[2] K. Froyum, S. Goepfert, J. Henrickson and J. Thorland, "Honeywell micro electro mechanical systems (MEMS) inertial measurement unit (IMU)," *Proc. Symp. Position Location and Navigation*, pp. 831-836, 2012.

[3] R. Lutwak, "Micro-technology for positioning, navigation and timing (Micro-PNT)," *DARPA*, 2016.

[4] B. Abbott and S. E. Lyshevski, "Signal processing in MEMS inertial measurement units for dynamic motional control", *Proc. IEEE Conf. Electronics and Nanotechnology*, pp. 309-314, 2016.

[5] S. E. Lyshevski, *MEMS and NEMS: Systems, Devices and Structures*, CRC Press, Boca Raton, FL, 2008.

[6] S. E. Lyshevski, *Mechatronics and Control of Electro-mechanical Systems*, CRC Press, Boca Raton, FL, 2016.

[7] S. E. Lyshevski, "Signal processing in cyber-physical MEMS sensors: Inertial measurement and navigation systems", *IEEE Trans. Industrial Electronics*, 2017.

[8] B. Scannell, "Sensor fusion approach to precision location and tracking for first responders," *Analog Devices Tech. Article*, 2016.

[9] D. K. Shaeffer, "MEMS inertial sensors: A tutorial overview," *IEEE Comm. Magazine*, vol. 51, issue 4, pp. 100-109, 2013.

[10] S. E. Lyashevskiy, "Robust nonlinear control of uncertain systems with state and control constraints," *Proc. IEEE Conf. Decision and Control*, New Orleans, Louisiana, vol. 2, pp. 1670-1675, 1995.

[11] S. E. Lyshevski, "State-space model identification of deterministic nonlinear systems: Nonlinear mapping technology and application of Lyapunov theory," *Automatica*, vol. 34, no. 5, pp. 659-664, 1998.

[12] C. R. Fuller, A. H. von Flotow, "Active control of sound and vibration," *IEEE Control Systems*, vol. 15, issue 6, pp. 9-19, 1995.

[13] S. E. Lyshevski, "Control of high performance induction motors: Theory and practice," *J. Energy Conversion and Management*, vol. 42, pp. 877-898, 2001.

[14] S. E. Lyshevski, "Diesel-electric drivetrains for hybrid-electric vehicles: new challenging problems in multivariable analysis and control," *Proc. IEEE Int. Conf. Control Applications*, Kohala Coast Island, Hawaii, pp. 840-845, 1999.

[15] S. E. Lyshevski and C. Yokomoto, "Control of hybrid-electric vehicles," *Proc. American Control Conf.*, Philadelphia, PA, vol. 4, pp. 2148-2149, 1998.

[16] A. Tzes and S. Yurkovich, "An adaptive input shaping control scheme for vibration suspension in slewing flexible structures," *IEEE Trans. Control Systems Technology*, vol. 1, issue 2, pp. 114-121, 1993.