



#2

Leo Simonovich

VP and Global Head, Industrial Cyber and Digital Security
Siemens Energy

Current contributor biography identifies Siemens Energy industrial-cyber leadership; this is an operating executive role, not a director-only profile. [Current-role source](#)

Direct business email and telephone: not publicly verified.

[LinkedIn profile](#) | [Named professional biography / public route](#)

Work base: Not established from reviewed sources. Actual work base, DC access and willingness require direct confirmation.

Recommendation and rationale

First-group qualification. ISA nominee; House-record comments, industrial policy, secure design and energy economics.

Research rank #2 - ISA core recommendations. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

FY2025 revenue EUR39.1bn, issuer release. Siemens Energy is separate from Siemens AG; do not substitute Siemens AG financials. [Source: www.siemens-energy.com](http://www.siemens-energy.com)

Proposed company benefit: Stronger oversight of power assets, supplier dependencies and security choices across asset lifecycles.

Proposed executive benefit: A policy and peer forum for advancing his industrial-security economics and secure-design priorities.

What This Recruit Could Add to ISA

Develop a capital-project case comparing secure design, retrofit expense and energy disruption. [Source: www.utilitydive.com](http://www.utilitydive.com)

Handbook connection: Tool H 57-59; B 37-40; K 66-68. Proposed output and benefits require agreement. [Source: www.nacdonline.org](http://www.nacdonline.org)

Introduction and next decision

Larry / ISA existing-prospect route. Larry identified Simonovich as a prospective member before the September board meeting; reconcile existing pipeline stage. [Source: mail.google.com](mailto:)

ISA to reconcile account status and route; then validate current remit, contribution, corporate payer and participation directly.

Policy history and board-selection fit

Policy / governance discussion: Own energy-policy remarks on public-private resilience, modernization incentives and AI infrastructure standards.

March 14, 2018 - Leo Simonovich: written comments on DOE modernization and cybersecurity. Makes the case for industry-government collaboration and a shared Charter of Trust for the industrial digital economy. Source: docs.house.gov

Written submitted comments verified; oral witness testimony is not established. Body describes historical Siemens; header uses Siemens Energy. Current employer scale is separate.

2018-11-07 - Driving security in an unsecure world - NIST conference presentation. Simonovich's presentation links industrial cyber risk to safety and production and outlines Charter of Trust principles, supplier requirements, certification and shared initiatives. Source: www.nist.gov

Historical Siemens presentation. Corporate principles and quoted colleagues remain corporate or separately attributed; no claim of regulatory adoption.

Benchmark: ISA recommendations, current ISA board practitioner profile, operating authority, company capacity, attributable policy work, concrete contribution, and portfolio balance. Corporate directorship alone does not determine priority.

Qualification status and ownership

Requirement	Evidence and remaining confirmation
Current role	Public role support; recheck directly before contact; direct confirmation pending.
ISA membership	Unknown current company/account and designated-representative status. Public board absence does not establish nonmembership.
Eligibility	Operating practitioner fit supported by research. ISA acceptance and employer designation pending.
Board feedback / introducer	Larry / ISA existing-prospect route. Introduction completion: not confirmed.
Corporate sponsorship	Published annual dues \$75,000; corporate payer, budget approver and written authorization not confirmed.
Executive interest	Not directly confirmed. Published interest in cyber topics is not membership interest.
Time / participation	Four meetings yearly, including two in Washington, DC and two virtual, plus agreed preparation. Availability, travel and term commitment not confirmed.
ISA output and benefits	Person-specific hypotheses documented; prospect and employer acceptance not confirmed.
Portfolio	Industry/expertise rationale assessed. Work base and DC access require direct confirmation.

ISA public board / meeting baseline | Bylaws | Published sponsorship

1631 owns researched case and source accuracy; ISA owns current membership/eligibility/introducer decision; employer/prospect must confirm funding, interest, availability and proposed output.

Image and contact provenance

Portrait: Portrait embedded beside named Leo Simonovich foreword, page 1. Cropped from authentic named portrait to focus on face and shoulders. **Source:** assets.siemens-energy.com

Company mark: Exact asset observed on named public source **Source:** www.siemens-energy.com

Attributable commentary and evidence ledger

11 / 10 substantive sightings recorded. Depth target met.

1. Building security into energy infrastructure by design is lower cost and more effective | Utility Dive

January 12, 2026 | Authored industry article [Source: www.utilitydive.com](http://www.utilitydive.com)

Argues security should be designed into energy infrastructure before construction, avoiding expensive retrofits and protecting reliability.

Attribution / limitation: Public position; confirm current relevance and company sponsorship interest.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

2. Minutes to Exploit-Months to Recover

August 3, 2026 | Authored industry article [Source: www.powermag.com](http://www.powermag.com)

Contrasts rapid exploitation with long industrial recovery; urges asset lifecycle planning and compensating controls for aging systems.

Attribution / limitation: Public position; confirm current relevance and company sponsorship interest.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

3. Energy leaders need to prepare for AI-powered cyber threats | World Economic Forum

July 24, 2026 | WEF article coauthored with Filipe Beato [Source: www.weforum.org](http://www.weforum.org)

Calls for energy asset visibility and prioritized remediation as AI accelerates threats; automation must support human expertise.

Attribution / limitation: Joint position; do not attribute every sentence to Simonovich alone.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

4. Cybersecurity for both data centres and their energy systems | World Economic Forum

May 5, 2026 | WEF article coauthored with Filipe Beato [Source: www.weforum.org](http://www.weforum.org)

Treats data-center resilience as a dependency problem spanning power, backup, cooling and physical access rather than IT systems alone.

Attribution / limitation: Joint analysis; no evidence of an ISA commitment.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

5. Why we need to power cyber resilience in the energy sector | World Economic Forum

May 9, 2025 | WEF article coauthored with Kesang Tashi Ukyab [Source: www.weforum.org](http://www.weforum.org)

Advocates collaboration across the energy ecosystem because suppliers and operators share cyber dependencies and reliability consequences.

Attribution / limitation: Coauthored; distinguish Siemens Energy from Siemens AG.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

6. The new cyber-threats to utilities: a Q&A with two experts | World Economic Forum

2020-05-22 | Speaker-labeled Q&A Source: www.weforum.org

Links IT/OT convergence with operational shutdown and safety consequences and calls for utility and equipment-manufacturer partnerships.

Attribution / limitation: Published position; no ISA interest or policy outcome is inferred.

ISA relevance: Sector expertise tied to physical business consequences.

7. AI can protect all energy firms from cyberattack. Here's how | World Economic Forum

2020-11-16 | Self-authored WEF article Source: www.weforum.org

Argues that weak links endanger the interconnected energy ecosystem and that detection must be feasible for smaller operators as well as large companies.

Attribution / limitation: Published position; no ISA interest or policy outcome is inferred.

ISA relevance: Economic feasibility and systemic resilience.

8. To minimize AI's cyber risks to energy infrastructure, start with the design phase | Utility Dive

2024-10-31 | Self-authored industry article Source: www.utilitydive.com

Discusses AI-related energy regulation and standards, industry cooperation and secure infrastructure design before future operating and compliance costs are locked in.

Attribution / limitation: Published position; no ISA interest or policy outcome is inferred.

ISA relevance: Specific policy and investment-design discussion.

9. Securing the energy and critical infrastructure sectors from cyberattacks - Atlantic Council

2021-12-13 event | Host recap with own attributed policy remarks Source: www.atlanticcouncil.org

Emphasizes sustained investment, public-private resilience partnerships and scenario preparation; identifies uncertainty in policies and funding for upgrading old equipment.

Attribution / limitation: Host recap; other panelists' views are excluded.

ISA relevance: Policy incentives and management decisions for industrial modernization.

10. EnergySource Innovation Stream: Artificial Intelligence-based monitoring for securing industrial IoT and the energy transition from cyberattacks - Atlantic Council

2021-10-04 event | Host recap with own attributed policy remarks Source: www.atlanticcouncil.org

Rejects treating technology adoption as a compliance exercise and urges investors to consider cyber exposure across the energy ecosystem.

Attribution / limitation: Host recap; other panelists' views are excluded.

ISA relevance: Economic incentives and practical adoption policy.

11. Driving security in an unsecure world - NIST conference presentation

2018-11-07 | Named government-hosted presentation **Source:** www.nist.gov

Simonovich's presentation links industrial cyber risk to safety and production and outlines Charter of Trust principles, supplier requirements, certification and shared initiatives.

Attribution / limitation: Historical Siemens presentation. Corporate principles and quoted colleagues remain corporate or separately attributed; no claim of regulatory adoption.

ISA relevance: Business-facing governance, practical controls or policy participation; ISA interest remains unconfirmed.