Alberta Emerging Reliability Risks 2025

Date: June 26, 2025

Version: 1

Classification: Public

Contents

1. Executive Summary

The Alberta Electric System Operator (AESO) is committed to maintaining reliability and security for the Interconnected Electric System[1] (IES) amid a rapidly evolving electricity landscape. The ongoing transition toward inverter-based resources (IBR), increased cyber threats, and the rising frequency of extreme weather events present complex challenges that necessitate proactive identification and management of emerging risks.

This report is developed as part of the Alberta Risk-Based Compliance Monitoring Program (ARCMP) system level risk process. The scope of this report identifies emerging reliability risks influenced by entities other than the AESO, informs the AESO's compliance monitoring priorities for the coming year, and provides guidance to applicable entities on key focus areas to support Alberta Reliability Standard (ARS) compliance efforts.

The five emerging reliability risks identified over the next year, which form the focus of this report, are:

1. **Frequency Stability** – declining inertia and governor response impact system frequency following disturbances.
2. **System Strength** – voltage stability and protection issues in weak-grid areas with high IBR penetration.
3. **System Security** – increased vulnerability due to grid digitization and cyber threat evolution.
4. **Extreme Weather Events** – reliability impacts from wildfires, heat waves, wind/ice storms, and other severe weather phenomena.
5. **Remedial Action Schemes (RAS)** – changes in system topology and operational conditions require robust testing and coordination of automated control schemes.

By integrating these identified risks with corresponding ARS requirements, this report provides a clear and transparent roadmap for AESO's targeted compliance monitoring and assurance activities. It ensures that AESO and applicable entity compliance efforts are aligned with the most pressing reliability priorities, supporting a resilient, secure, and sustainable IES.

2. Emerging Reliability Risks

2.1 Frequency Stability

Risk Summary

The IES is experiencing a decline in inertia and governor response as synchronous generation is displaced by IBRs. This trend reduces the effectiveness of primary frequency response and increases the risk of under-frequency load shedding (UFLS), as well as emerging over-frequency risks during periods of high exports or sudden industrial load drops.

Mitigation Actions

Applicable entities play a critical role in mitigating frequency stability risks through:

[1] As defined by the Electric Utilities Act, SA 2003, c E-5.1

- Participating in the design, implementation, and assessment of UFLS programs to ensure alignment with system needs and adapting to changes in system inertia and frequency performance.
- Maintaining voltage and reactive power control in accordance with AESO directives to support system voltage stability, indirectly contributing to frequency control.
- Notifying the AESO when voltage or reactive power schedules cannot be maintained to ensure operational awareness and coordination during abnormal grid conditions.

ARS Alignment

- **PRC-006-AB-3**: Requires applicable entities to participate in the design, implementation, and assessment of UFLS programs.
- **VAR-002-AB-4.1**: Requires generators to maintain voltage and reactive power output according to system needs, indirectly supporting frequency stability.

2.2 System Strength

Risk Summary

System strength refers to the grid's ability to maintain voltage stability and ensure proper operation of protection systems, especially during fault conditions. In areas with high penetration of IBRs, such as southern Alberta, reduced system strength can lead to slower voltage recovery following faults and increase the risk of protection misoperation. These weak-grid conditions complicate reliable operation and may result in the need for operational constraints or infrastructure reinforcement.

Mitigation Actions

Applicable entities contribute to mitigating system strength risks through:

- Maintaining voltage and reactive power control in accordance with AESO directives to support system voltage stability, particularly in areas with reduced synchronous support.
- Ensuring that facility ratings accurately reflect equipment capabilities critical for reliable operation in weak-grid conditions and ensuring proper protection coordination.

ARS Alignment

- **FAC-008-AB-3**: Requires facility ratings to accurately reflect equipment capabilities, essential for maintaining operational integrity in weak-grid areas.
- **VAR-002-AB-4.1**: Requires generators to maintain voltage and reactive power output according to system needs, supporting voltage stability in regions with high IBR concentrations.

2.3 System Security

Risk Summary

As the IES becomes more digitized and interconnected, the risk of cyber threats, including phishing, ransomware attacks, in addition to supply chain issues, continues to grow. Applicable entities operating critical infrastructure face exposure to attacks targeting operational technologies, business systems, and third-party vendors. A successful cyberattack can disrupt visibility, control, or operations, potentially leading to reliability events or cascading impacts.

Mitigation Actions

Applicable entities can strengthen system security through:

- Implementing a cybersecurity governance framework to establish baseline security policies and ensure oversight.
- Conducting personnel risk assessments, cybersecurity training, and access control to minimize insider threats and unauthorized access.
- Establishing and maintaining electronic security perimeters and access controls to protect critical cyber assets from external intrusion.
- Applying physical security protections for bulk electric system (BES) cyber systems.
- Implementing baseline system hardening, patch management, malware protection, and monitoring controls to reduce system vulnerabilities.
- Maintaining and testing recovery plans for cyber assets to support continuity in the event of a cybersecurity incident.
- Applying configuration change management and integrity monitoring to detect unauthorized or harmful modifications.
- Protecting sensitive BES cyber system information to prevent data leakage or misuse.
- Managing supply chain cybersecurity risk for applicable entities by applying controls to vendor management and procurement processes.
- Conducting physical security risk assessments and implementing security enhancements at critical substations to mitigate physical threats to reliability.

ARS Alignment

- **CIP-003-AB-5 and CIP-003-AB-8**: Baseline cybersecurity policy and governance.
- **CIP-004-AB-5.1 and CIP-004-AB-7**: Personnel training, background checks, and access management.
- **CIP-005-AB-7**: Electronic security perimeters and access control.
- **CIP-006-AB-5**: Physical protections for BES cyber systems.
- **CIP-007-AB-5**: Security management controls including patching, anti-malware, and monitoring.
- **CIP-009-AB-5**: Recovery plans for BES cyber systems.
- **CIP-010-AB-4**: Change management and configuration monitoring.
- **CIP-011-AB-1 and CIP-011-AB-3**: Protection of sensitive BES cyber system information.
- **CIP-012-AB-1**: protects the confidentiality and integrity of real-time assessment and monitoring data between control centers.
- **CIP-013-AB-2**: Supply chain cybersecurity risk management for entities with medium or high impact BES Cyber Systems.
- **CIP-014-AB-2**: Physical security risk assessments and protections for transmission substations critical to IES reliability.

2.4 Extreme Weather Events

Risk Summary

The IES is increasingly exposed to extreme weather conditions such as wildfires, prolonged heat waves, and severe wind or ice storms. These events can cause equipment damage, forced outages, deratings, and access issues. They also increase operational complexity and elevate the risk of widespread system impacts. Enhancing preparedness and infrastructure resilience is essential for managing these risks.

Mitigation Actions

Applicable entities support extreme weather readiness and system resilience through:

- Maintaining blackstart capability and supporting restoration procedures to ensure system recovery following widespread outages caused by severe weather events.
- Developing and maintaining emergency operating plans to address capacity and energy emergencies, which includes procedures for coordination during extreme environmental conditions.

ARS Alignment

- **EOP-005-AB-3**: Requires blackstart capability plans to restore the system after a widespread outage, including during adverse weather conditions.
- **EOP-011-AB-1**: Requires emergency operations plans to address capacity and energy emergencies, including coordination during extreme weather events.

2.5 Remedial Action Schemes (RAS)

Risk Summary

RAS are automated control schemes that execute predefined corrective actions to prevent cascading outages or system instability. As the IES becomes more complex, evolving system topology and operating conditions may reduce the effectiveness of existing RAS if not routinely tested, coordinated, and maintained. Improper settings or lack of coordination can result in unintended consequences or missed corrective actions.

Mitigation Actions

Applicable entities that own or operate RAS equipment are expected to:

- Analyze and correct RAS misoperation to ensure RAS operate as intended during system disturbances.
- Coordinate with the AESO and other affected entities when modifying or retiring RAS to maintain correct protection system interaction and avoid unintended consequences.
- Maintain accurate documentation and configuration control for RAS to support traceability of scheme logic and system response behavior.
- Train operations and engineering personnel on RAS functionality and responsibilities to ensure appropriate actions are taken during system events involving RAS.
- Implement and follow maintenance programs to test and validate RAS performance on a defined schedule.

ARS Alignment

- **PER-005-AB-2**: Requires personnel trained in the operation of RAS, where applicable to their responsibilities.
- **PER-006-AB-1**: Requires personnel trained in the protection system operation, including RAS.
- **PRC-001-AB3-1.1(ii)**: Requires coordination of protection systems, including RAS, to ensure correct operation during system events.
- **PRC-004-WECC-AB1-1**: Requires analysis and corrective action following protection system misoperation, which includes RAS failures or false triggers.
- **PRC-004-AB2-1**: Addresses the identification and correction of protection system and RAS misoperation.
- **PRC-005-AB2-6**: Requires that protection systems, including RAS, are properly maintained.

3. ARS Risk Mapping

Emerging Risk	Applicable ARS	Requirement(s)
Frequency Stability	1) PRC-006-AB-3 2) VAR-002-AB-4.1	1) R8, R9, R10 2) R1, R2, R3
System Strength	1) FAC-008-AB-3 2) VAR-002-AB-4.1	1) R6 2) R1, R2
System Security	1) CIP-003-AB-5 and CIP-003-AB-8 2) CIP-004-AB-5.1 and CIP-004-AB-7 3) CIP-005-AB-7 4) CIP-006-AB-5 5) CIP-007-AB-5 6) CIP-009-AB-5 7) CIP-010-AB-4 8) CIP-011-AB-1 and CIP-011-AB-3 9) CIP-012-AB-1 10) CIP-013-AB-2 11) CIP-014-AB-2	1) R2 2) R2, R3, R4, R5, R6 (CIP-004-AB-7 only) 3) R1, R2, R3 4) R1, R2, R3 5) R1, R2, R3, R4 6) R1, R2, R3 7) R1, R2, R3 8) R1, R2 9) R1 10) R1, R2, R3 11) R4, R5, R6
Extreme Weather Events	1) EOP-005-AB-3 2) EOP-011-AB-1	1) R1, R5, R9, R12, R14 2) R1, R4
RAS	1) PER-005-AB-2 2) PER-006-AB-1 3) PRC-001-AB3-1.1(ii) 4) PRC-004-WECC-AB1-1 5) PRC-004-AB2-1 6) PRC-005-AB2-6	1) R1, R3 2) R1 3) R1, R2, R3 4) R1, R2, R3 5) R1, R2, R3 6) R1, R2, R3, R4, R5

4. References

- AESO, *Alberta 2023 Emerging Reliability Risks*, posted: July 2024, available at: www.aeso.ca.
- AESO, *AESO 2023 Reliability Requirements Roadmap*, posted: March 2023, available at: www.aeso.ca.
- AESO, *Alberta Risk-Based Compliance Monitoring Program*, version 1.2, posted: February 2025, available at: www.aeso.ca
- AESO, *Complete Set of Alberta Reliability Standards*, posted: October 2024, available at: www.aeso.ca.
- NERC, *2025 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan*, Version 2.0, November 2024, available at: www.nerc.com.
- WECC, *2024 Western Interconnection Reliability Risk Report*, available at: www.wecc.org.