



S/AIC: Balancing Safety & Availability of Operational Technology

Securing BAS White Paper Series 2 of 6

CONTACT INFORMATION

877.444.5622 

info@kmccontrols.com 

www.kmccontrols.com 

19476 Industrial Drive, New Paris, IN 46553 



Table of Contents

Executive Summary	1
Introduction	1
The Shift from CIA to S/AIC	2
Why Availability Comes First in OT	3
Conclusion	4



Executive Summary

This white paper introduces the Safety/Availability, Integrity, & Confidentiality (S/AIC) set of principles to rethink OT cybersecurity priorities. It contrasts traditional IT models with the operational realities of building systems, provides a foundational understanding for both OT and IT audiences, and explains why S/AIC should be supported by practical controls such as asset awareness, approved remote access, incident reporting, and resilient recovery planning.

Introduction

Cybersecurity has become an increasingly critical focus for operational technology (OT) environments as industry practices evolve and systems grow more interconnected. As building automation systems (BAS) become increasingly connected to enterprise IT networks and cloud-based services, the risk of cyber threats impacting critical building functions grows significantly.

Traditional IT security is designed for data protection. In OT, however, system unavailability or compromised process integrity can have far more immediate consequences; directly affecting human safety and the resilience of critical infrastructure.

This white paper introduces the S/AIC principles as a practical way to evaluate OT cybersecurity needs and guide security decisions that align with the realities of building operations. In practice, these decisions should be documented through owner requirements, service provider procedures, and system design choices, protecting safety and uptime are without leaving integrity and confidentiality unmanaged.

This paper lays the foundation for the rest of the series:

- **Paper 1** introduces cyber hygiene; the human layer of security that underpins all technical controls in this series.
- **Paper 3** applies the S/AIC principles to BACnet network security best practices for OT teams.
- **Paper 4** helps IT professionals understand how BACnet networks and OT devices differ from typical IT systems.
- **Paper 5** presents decision making principles for choosing between BACnet/SC, KMC Dome, or a hybrid model.
- **Paper 6** provides a deep dive into when and why KMC Dome may be a better or complementary solution.

The Shift from CIA to S/AIC

In traditional IT security models, the CIA triad (Confidentiality, Integrity, & Availability) represents the guiding principles for security of data. Confidentiality usually takes precedence, especially in systems managing sensitive data such as personal records or financial transactions.

In contrast, OT systems prioritize continuous, reliable operation of physical processes. Ensuring safety and maintaining uptime are paramount; for example, losing control of a ventilation system during extreme weather could endanger occupants or damage equipment. For this reason, the OT community adopted a modified model: the S/AIC tetrad. This reorders the priorities and adds explicit focus on safety as it relates to operational impact:

- **Safety:** System operations must not be compromised to the point that human or equipment safety is jeopardized.
- **Availability:** The system must always be accessible to operators.
- **Integrity:** The data and commands in the system must not be altered in unauthorized ways.
- **Confidentiality:** Confidential data must be protected, but not at the expense of availability or safety.

This shift highlights a key tension in OT security: security controls must not interfere with critical operations. For example, an overzealous firewall rule could inadvertently disable HVAC systems in a hospital, directly impacting patient safety and facility operations.

Applying S/AIC in real BAS environments, therefore, means more than choosing the right technology. It also means identifying critical assets, documenting zones and conduits where practical, approving remote connections, assigning responsibility for incident escalation, and verifying that backup and recovery steps support safe operations.

Why Availability Comes First in OT

The S/AIC principles help align cybersecurity priorities with the real-world needs of building automation. Rather than applying IT principles directly to OT environments without adaptation, organizations should assess threats and solutions through the lens of safety, availability, integrity, and confidentiality, and then translate those priorities into documented owner expectations, service practices, and system safeguards.

By internalizing these priorities, OT teams are better prepared to evaluate security technologies, balance operational risk, and collaborate effectively with IT stakeholders. At a minimum, this collaboration should clarify who approves remote access, how accounts and changes are controlled, how suspicious events are reported, and how critical systems are restored after failure.

Conclusion

The S/AIC principles help align cybersecurity priorities with the real-world needs of building automation. Rather than applying IT principles directly to OT environments without adaptation, organizations should assess threats and solutions through the lens of availability, integrity, and confidentiality; with a practical understanding of what 'security' really means for OT.

By internalizing these priorities, OT teams are better prepared to evaluate security technologies, balance operational risk, and collaborate effectively with IT stakeholders.

The next paper in this series will show how to apply these concepts to harden BACnet networks while maintaining the operational flexibility OT teams need.

