DERISK CRQ · LEVEL 4 · EVIDENCE-GRADE · CHIEF RISK OFFICER

Risk Transfer Evidence Bundle — 2026 Renewal

Generated by DeRISK CRQ on the DeRISK™ Intelligence Platform.

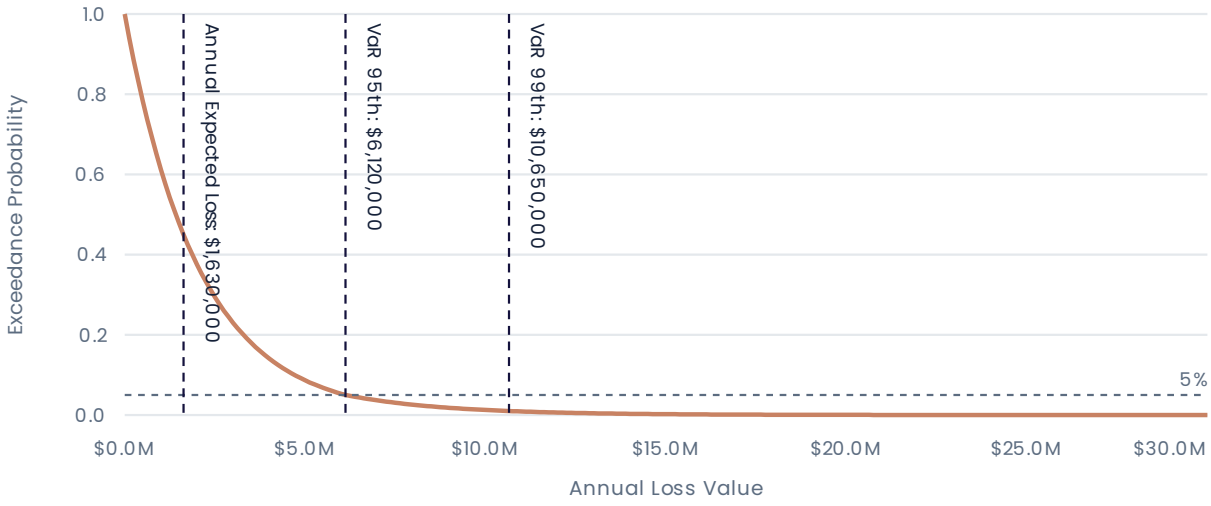
Entity: Veltrane Digital **Facility:** Example Facility 1 **Scope:** Facility **Level:** 4 · Evidence-Grade
Inputs provided: Oct 27, 2026 **Report generated:** Oct 27, 2026 **Cadence:** Renewal cycle

Exhibit set for broker and underwriter: exposure schedule, modeled loss picture, risk quality evidence, and the improvement narrative.

EXHIBIT 1 · MODELED LOSS PICTURE — LAYER-SIZING ANCHORS

METRIC	LOSS	DAYS OF REV.	% OF REVENUE
Annual Expected Loss	**$1,630,000**	**0.5**	**0.14%**
VaR 95th (1-in-20) — attachment anchor	$6,120,000	1.86	0.51%
VaR 99th (1-in-100) — limit-sizing anchor	$10,650,000	3.24	0.89%

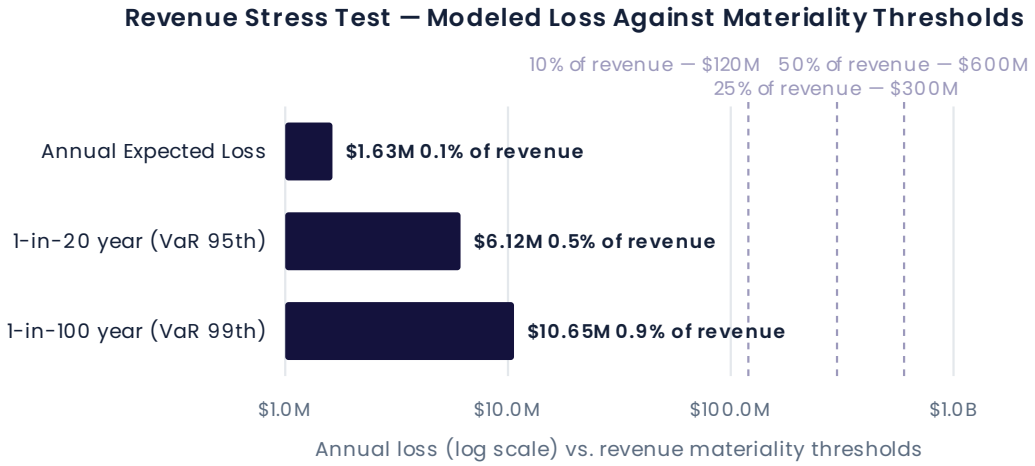
Facility Annual Loss Exceedance Curve



The facility exceedance curve has a 5% annual probability of exceeding $6.12M (VaR 95th) and a 1% annual probability of exceeding $10.65M (VaR 99th). The curve shape between and beyond these anchors is illustrative; Annual Expected Loss is shown for reference.

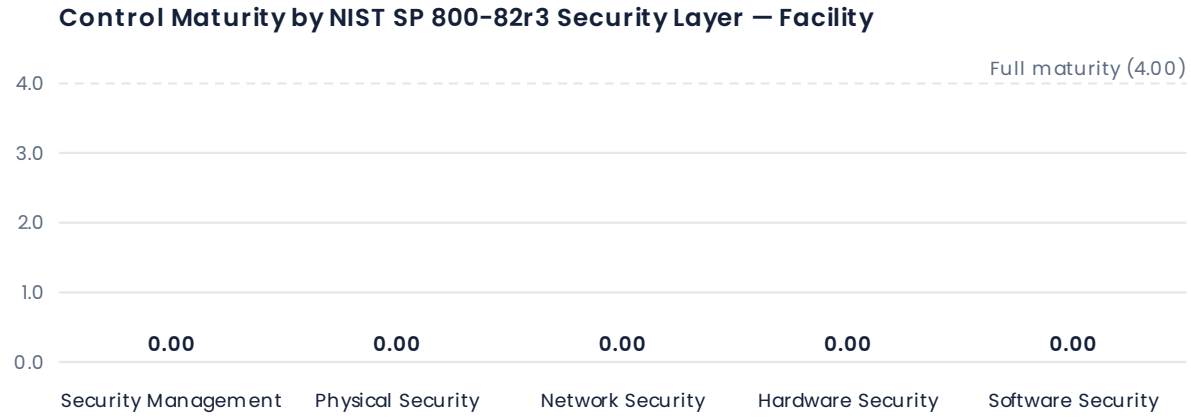
© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

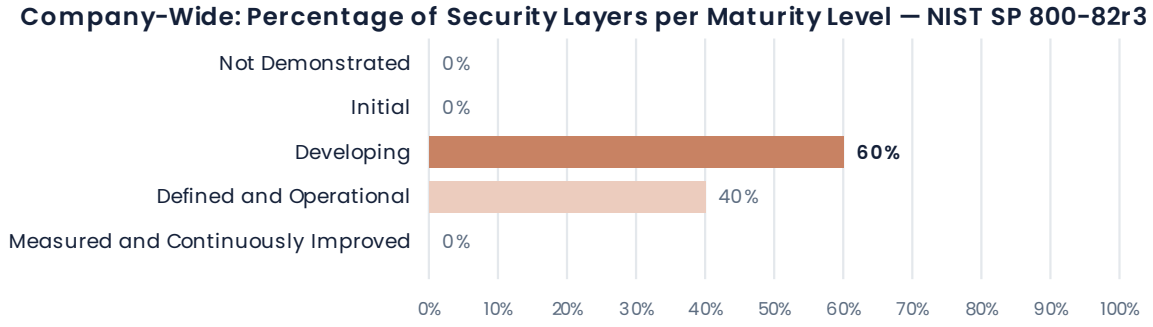
EXHIBIT 2 · SEVERITY REALISM



All displayed modeled loss measures are **below** the lowest revenue materiality threshold, set at 10% of annual facility revenue. The 1-in-100-year loss equals **0.89%** of annual facility revenue.

EXHIBIT 3 · RISK QUALITY EVIDENCE

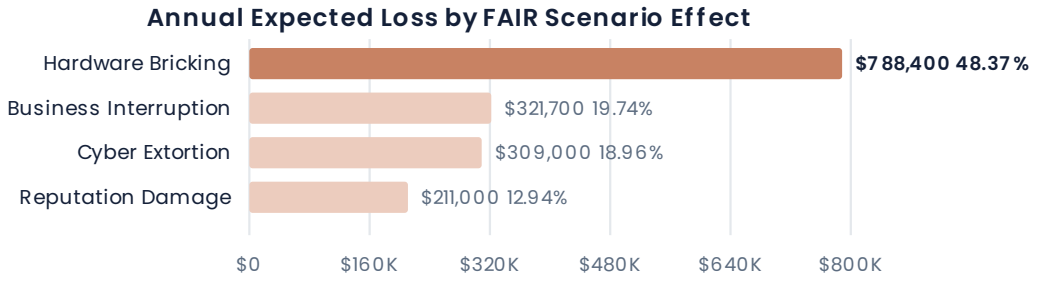




Overall control maturity is **0.00 of 4.00 (Not Demonstrated)**. The assessment could not credit maturity in any of the five OT security layers for Example Facility 1 because the information provided contained only identifiers and financial impact figures, with no operational or technical evidence of OT-specific controls. This result reflects a lack of available evidence rather than a confirmed absence of protections, and submitting OT governance, network, and asset documentation would enable a meaningful re-evaluation. Comparable industry peer data are not available. In the company-wide assessment, 60% of assessed security layers are rated Developing.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

EXHIBIT 4 · SCENARIO DECOMPOSITION



The largest FAIR scenario Effects are **Hardware Bricking** and **Business Interruption** — together 68.1% of facility Annual Expected Loss.

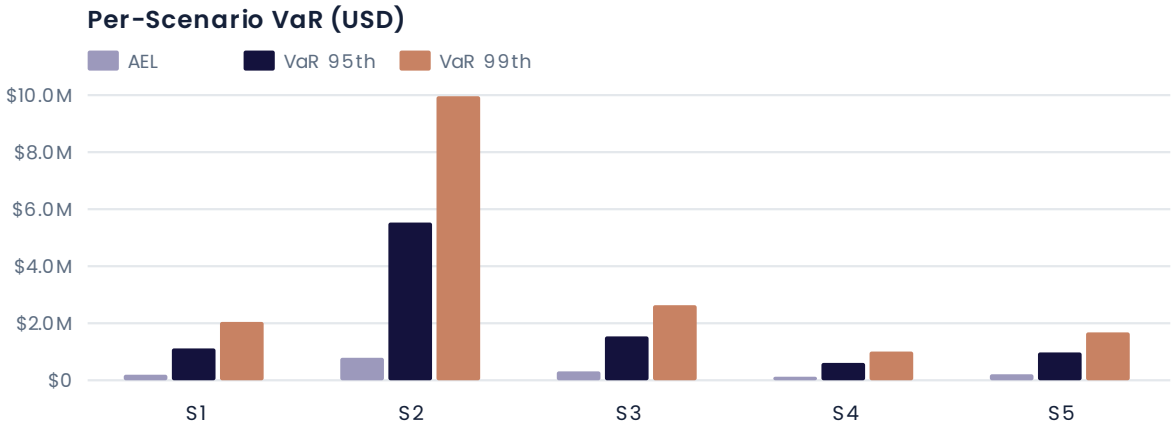
EXHIBIT 5 · FAIR SCENARIO ANALYSIS

5.1 FAIR Scenario Register

ID	THREAT	ASSET	METHOD	EFFECT	RELEVANCE
S1	**Nation-State**	Business Process Generating Revenue	Remote Service Exploitation	Business Interruption	Unpatched Modicon PLCs with known remote-code-execution flaws, reachable via connected HMIs and a protocol gateway, give nation-state actors a viable path to disrupt the entire control layer simultaneously.
S2	**Sabotage Actors**	Physical Assets & Facilities	Malware	Hardware Bricking	A flat, homogeneous network of unpatched Modicon PLCs—all sharing the same critical vulnerabilities and reachable from HMIs and a protocol gateway—enables a sabotage actor to brick every controller in a single coordinated attack.
S3	**Cyber Criminals**	Business Process Generating Revenue	Ransomware without Data Exfiltration	Cyber Extortion	Nine unpatched Modicon PLCs interconnected without segmentation, accessible through Windows-based HMIs, let ransomware actors lock the entire production floor and leverage costly OT recovery time to pressure payment.
S4	**Privileged Insider**	Product or Service	Data Corruption	Business Interruption	Insiders with legitimate HMI access can use authorized engineering tools to push corrupted logic to all nine interconnected, unpatched Modicon PLCs, causing process upsets or shutdowns without needing to exploit any vulnerability.
S5	**Hacktivists**	Business Process Impacting Third-Party Revenue	System Outage	Reputation Damage	Publicly documented, unpatched vulnerabilities across all Modicon PLCs—reachable via HMIs and a protocol gateway—lower the barrier for hacktivists to halt operations and publicize the outage, causing reputational and supply-chain damage.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

5.2 Per-Scenario VaR and Contribution



SCENARIO	AEL	VAR 95TH	VAR 95TH CONTRIBUTION	VAR 99TH	VAR 99TH CONTRIBUTION
S1	$196,300	$1,118,000	11.44%	$2,047,000	11.81%
S2	$788,400	$5,530,000	56.57%	$9,960,000	57.47%
S3	$309,000	$1,541,000	15.77%	$2,633,000	15.19%
S4	$125,400	$610,000	6.24%	$1,010,000	5.83%
S5	$211,000	$976,000	9.98%	$1,682,000	9.70%

EXHIBIT 6 · METHODOLOGY AND TRANSPARENCY

6.1 Data Sufficiency and Confidence

ASPECT	ASSESSMENT
Data sufficiency	Partial. The assessment received detailed, well-reasoned scenario narratives and several usable financial anchors (hourly revenue loss, forensic cost, equipment replacement value, facility revenue), which support a directional analysis. However, no empirical frequency data, control-effectiveness measurements, historical incident records, downtime durations, or insurance and recovery-cost figures were provided, so frequency, vulnerability, and loss-magnitude parameters are substantially assumption-driven.
Confidence level	Moderate. Results are directionally reliable for prioritization and decision support, grounded in company-provided financial anchors and a stable 100,000-iteration simulation, but they depend materially on inferred frequency, vulnerability, and downtime assumptions. Reasonable changes to these inferred inputs could shift absolute VaR figures, though the relative ranking of dominant scenarios is expected to remain stable.

6.2 Financial and Contextual Inputs

INPUT	VALUE
Company name	Veltrane Digital
Industry	Datacenters
Geography	North America and Europe
Number of facilities	14
Average cost per hour of Cybersec Forensic Services during a loss event	$450
Estimated Revenue loss per hour during a downtime event	$4,500
Total cost of equipment that could be damaged in a loss event	$50,000,000

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

INPUT	VALUE
Annual facility revenue	$1,200,000,000
Annual company revenue	$187,600,000,000
Revenue loss per hour of downtime	$4,500
Equipment replacement value	$50,000,000
Critical assets in the facility topology	241
Target assets of the exploitable attack paths	2
Highly feasible exploitable attack paths analyzed	16
Applicable MITRE ATT&CK techniques in the exploitable paths (inferred from the topology)	6
Potentially applicable CVEs in the exploitable paths (inferred from the topology)	11

6.3 Assumptions Register

1. The likelihood and frequency of cyberattacks against the facility had to be estimated from industry knowledge because no record of past security incidents or attempted attacks was provided.
2. The effectiveness of current security controls and defenses had to be assumed because no information on existing protections or security maturity was provided.
3. The duration of operational outages following an incident had to be estimated because no information on recovery times or past downtime was provided.
4. The broader financial consequences such as regulatory penalties, reputational harm, and safety or environmental costs had to be estimated because no figures for these were provided.
5. The share of physical equipment that could be permanently damaged in a destructive event was estimated from the overall equipment value provided, as no detail on individual asset exposure was available.

6.4 Limitations

- Because the results rely substantially on estimated attack frequencies, control effectiveness, and recovery times, the figures are best used to prioritize and compare risks rather than as precise loss forecasts; providing incident history, control assessments, and recovery-time records would significantly sharpen them.
- The loss estimates cover direct operational and recovery costs well but treat regulatory, reputational, and safety or environmental consequences as approximations; information on contractual penalties, insurance coverage, and past consequence costs would make these figures more reliable.
- The destructive-event scenario, which drives the worst-case results, depends heavily on an assumed level of equipment damage; a detailed inventory of critical control hardware and its replacement lead times would materially improve confidence in the upper-end loss figures.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.