International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Digital Twin-Enabled Stress Testing of Financial Controls in ERP Environments: A Framework for Systemic Resilience

Vijaya Bhaskar Reddy Saadhu

Abstract: Digital twin technology used in the enterprise resource planning landscape opens a door to validation of financial controls in real time and under extreme dynamic circumstances that cannot be accomplished using customary audit environments. Customary validation of controls is not dynamic and is performed as a snapshot of controls operating in conformance to design specifications. These methods may neglect to consider the combined presence of multiple stressors, including market liquidity crises, coordinated fraud as a service, cascading system failures, and dramatic regulatory changes. The creation of high-fidelity representations of the financial processes, transaction flows, authorization hierarchies and control rules enables the simulation of adversarial and edge cases in a safe environment without risking production systems. It defines the steps to perform data extraction, governance, process and control rule modeling, stress scenarios, privacy-preserving data management, dynamic model validation via backtesting and expert parameter calibration. It also identifies the performance metrics based on resilience, such as fraud detection rates, risk mitigation rates, throughput improvement rates, and compliance assurance rates, which are quantitative measures of control efficacy that utilize simulation outputs. In addition to supporting internal governance processes, these metrics can help satisfy regulatory compliance needs. Hybrid simulation and audit techniques address known limitations of simulation in risk management, such as the high cost of implementation, the decay of models used in such practice, the privacy concerns of regulatory regimes, and resistance from audit and finance functions. As a continuous improvement discipline, the digital twin framework helps organizations proactively identify and improve latent control weaknesses in increasingly complex enterprise risk environments before they can cause operational failure rather than merely detect when operational failure occurs (or is imminent).

Keywords: *Digital Twin, Enterprise Resource Planning, Financial Control Validation, Stress Testing, Systemic Resilience*

1. Introduction

Global transaction flows, multi-jurisdictional regulatory requirements, and technology interdependencies, not to mention evolving fraud vectors, are creating increasingly complex business operations. These are making it difficult for customary financial control validation techniques to provide an appropriate level of assurance. Static, point-in-time control testing has long been the core model of conventional audit practice. Static control testing assesses the design and operating effectiveness of controls at discrete points in time. This relates to a broader limitation that it is unable to assess the control performance of dealing with dynamic compounding stressors [1], a limitation that is not merely theoretical. Control failures resulting from poor stress scenario coverage have resulted in regulatory penalties and institutional failures throughout the financial sector.

Independent Researcher, USA

The experience of many financial institutions suggests that the testing of these controls and validation of their effectiveness must be re-evaluated. Asset-liability management controls may have been functionally adequate under normal conditions, as was seen during the rapid hikes in interest rates during 2022 and 2023; they were structurally inadequate under stress [2]. Along similar lines, anti-money-laundering control frameworks that passed periodic regulatory inspections were not able to detect coordinated long-running money laundering schemes because the frameworks had never been subjected to adversarial stress testing that explored the boundaries of detection [3].

Digital twin technology offers a conceptual solution. Digital twins were first applied to tightly controlled aerospace and manufacturing environments where real-time, highly accurate virtual replicas of a physical asset were required and have now moved on to advanced organizational systems, including supply chains and healthcare

delivery networks and enterprise information systems [4]. A digital twin of an ERP financial environment is a high-fidelity virtual representation of financial processes, transaction workflows, and control logic, which allows extreme scenarios such as market gyrations, fraud profiles, and regulatory changes to be simulated without any risk to the organization's production systems.

This article makes three contributions to the literature on financial control validation and enterprise risk management. It provides a systematic methodology for the implementation of enterprise resource planning (ERP)-based digital twins for financial control stress testing, thereby extending previous digital twin studies from an operational efficiency focus to financial governance. Second, it provides a framework that connects digital twin simulation capabilities and resilience metrics to quantify the effectiveness of controls and justify the investment in digital twin infrastructures. Third, it addresses the regulatory, privacy, and governance constraints that differentiate controls from other digital twin use cases, offering practical guidance for overcoming those constraints while retaining the analytical power of digital twins.

2. Digital Twin Architecture for ERP Financial Environments

An ERP digital twin is a digital twin, existent in accordance with its definition as always up-to-date, high-fidelity virtual models of a given physical object or process that are employed for real-time monitoring, predictive modeling and iteration optimization [5]. Digital twins in manufacturing and industrial setups are sensor-based digital representations that build from telemetry data via a continuously updated digital model. There is, however, a meaningful methodology gap in applying this architecture to ERP financial environments due to the financial controls under regulatory scrutiny, data confidentiality, and auditability generally not found in industrial contexts.

There are five functional layers that compose the ERP financial digital twin, which are processes that interact in real-time with its physical ERP counterpart. The physical ERP layer includes the data capture, the rule-based controls, the segregation of duties (SoD), and the system of record for financial transactions. The data extraction layer bridges the operational and virtual layers, continuously extracting operational data, transaction-level logs, user access events, system configuration status, and external risk monitoring. The virtual simulation layer refers to the digital twin model itself, an executable model of financial processes, control rules, approval hierarchies, and exception management procedures that reflects the behavior of the operational system under normal and stressed conditions [6].

These can be combined in the scenario configuration layer to simulate transaction spikes, market shocks, fraud patterns, regulatory change and multi-factor stresses. The analysis, feedback, and recommendations layer then translates these results into risk-based control efficacies, performance measures, and remediation recommendations, feeding back into the digital twin or the operational ERP instance.

An important aspect in ERP digital twin architecture is the calibration of model fidelity. In physical systems, sensor data provides an objective ground truth measure of system state. On the other hand, financial process models must be created from transaction, workflow, business rule, and configuration data that may be incomplete, inconsistently documented, or subject to informal operational exceptions that reside outside of the system configuration [7]. The digital twin will contain intrinsic inaccuracies that must be controlled for via backtesting and subject matter expert validation. The usefulness of the information and analysis provided by the digital twin is proportional to the accuracy of the digital twin control, which will be at least 95%. Below this threshold the risk of false negatives in stress testing means a dangerous breach of control assurance.

At the same time, process mining techniques (i.e., discovering process models from event logs) represent a methodological approach that can support the development of ERP-based digital twins. They exploit data created in the system (as opposed to documentation), which results in a more accurate and complete process model than documentation-based methods (see [8]). Because process documentation typically lags behind real-world processes in financial control environments, using process mining to create the digital twin model allows it to be always verifiably correct in the sense that it accurately represents how controls actually

operate rather than how they are theoretically designed to operate.

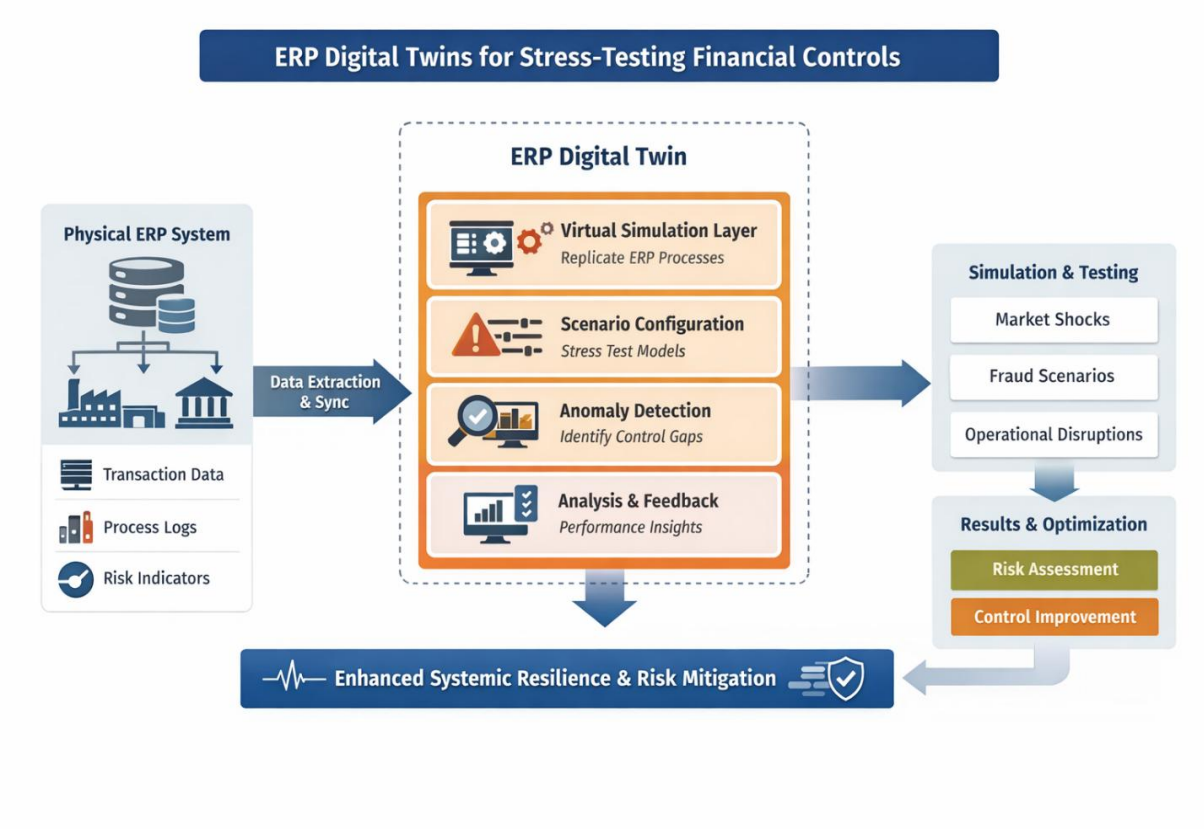

Fig. 1. ERP digital twin framework

3. Testing Financial Controls: Rationale and Scenario Design

The rationale for stress testing is a structural one: Controls which work well under normal circumstances can fail catastrophically in a predictable manner under stress, and no control testing regime can prospectively identify these stress failure modes. Stress testing has long been legislated in banking regulation on the grounds that capital adequacy and liquidity controls, which are generally effective in benign macroeconomic conditions, can break down catastrophically under the pressure of correlated stress in financial markets. The same logic applies broadly to operational financial controls.

Financial stress scenarios for the ERP control environment can be classified into four categories. Market and liquidity scenarios test cash position management, authorization of large-value transactions, and trading limits, with reduced time for investigation while still allowing for a large number of transactions to be processed. When organizations are forced to process abnormal volumes of transactions under time pressure, the usual authorization and exception procedures, exception queues and escalation procedures can become clogged, overflowed, or stalled, thus providing weaknesses that can be exploited by attackers [2]. Fraud and collusion cases test the limits of the preventive and detective controls , by creating conditions under which the fraud patterns are generated in the simulated environment. More advanced frauds involve collusion between people who have complementary access rights, taking advantage of the seams between effective individual controls and escaping detection since each control is functioning as intended, even though the ensemble is not [3].

System failure/cascade scenarios assess the recovery of controls when components of the integrated technology environment partially fail, data quality deteriorates, or processing delays occur. The

effectiveness of controls in the integrated technology environment is generally dependent on the integration with surrounding or peripheral systems (e.g., banking systems, payment processors, regulatory reporting systems, data warehouses, etc.). Digital twin simulation can be used to model integration failures or control logic behavior and possible control breakdowns when data feeds are late, missing, or corrupted. Regulatory change scenarios can be used to test control robustness against regulatory changes hypothesized to be both possible and plausible, such as new transaction limits, new data retention requirements, and new reporting periods, and gaps can be identified prior to regulatory implementation, rather than during a post-implementation audit.

The scenario should be specified at three levels of granularity: (1) parameters of the scenario (e.g., transaction volumes, size of price movements, time windows, and data quality degradation rates) at which the stress test is performed; (2) anomaly injection specifications that define the parameters of adversarial patterns (i.e. fraud schemes, collusive behaviors, and system manipulations) to be injected into the simulation; and (3) scenario administration specifications. Multi-factor combinations of stressors (effectively, multiple stressors occurring simultaneously) are the most challenging simulator of control resilience, as most control failures in the real world are due to multiple interacting stressors rather than single factor shocks [9]. Scenario specifications can ease reproducibility by making it possible for organizations to repeat stress tests as control conditions change and to compare results across different testing settings.

Scenario Category	Stress Condition	Control Domain Tested	Key Evaluation Dimension
Market & Liquidity Stress	Compressed decision windows, elevated transaction volumes	Cash management, authorization thresholds	Control response time under volume surge
Fraud & Collusion	Coordinated exploitation of complementary access rights	Segregation of duties, detective controls	Ensemble control failure detection rate
System Failure & Cascade	Partial failures in integrated peripheral systems	Data-dependent controls, reconciliation	Control degradation under data feed disruption
Regulatory Change	Modified thresholds, new reporting mandates	Compliance controls, reporting workflows	Compliance gap identification lead time

Table 1: Stress Scenario Categories and Control Evaluation Dimensions for ERP Financial Environments [9]

4. Implementation Methodology and Governance Framework

A financial control stress testing ERP digital twin can be realized by following a managed process, which sequentially covers the areas of data management, digital twin modeling, validation, security, and governance. The approach is a good guide for organizations to follow.

The first step is to collect and analyze the data. The digital twin models of the well-functioning systems will include full and accurate data regarding transaction master files, process flow documents, control rules, system configuration files (e.g., access rights, segregation of duties matrices), and event logs regarding the history of the executed and unexecuted system actions [8]. Data extraction should include reconciliation checks to ensure completeness and accuracy against the source systems and data governance principles whereby the extracted data accurately reflects the operational configuration at the time of extraction, rather than the historical state that could misrepresent current control arrangements.

The second phase of transaction modeling and control rules takes data from phase one, producing an executable model of financial transactions. It models transaction flow control from the beginning of a transaction through to authorization, processing, and settlement, with control at each decision point. In addition to business rules that are documented and communicated in practice, implicit business rules are discovered through iterating with control owners and process managers and applying process mining techniques to the event log data from

the information system [7]. The management of control points can include preventive controls designed to block an unauthorized transaction at the time of execution and detective controls searching for exceptions after the fact.

In phase three, stress testing scenarios are defined based on the baseline created in phase one, using the four main types of scenarios detailed above. The configuration tooling should allow scenarios to be reproduced precisely at the technical level, but this should not be at the cost of usability by non-technical business users familiar with domain stress conditions. Scenario documentation and standardization serve the dual purpose of reproducibility and comparison to past test runs. Multi-factor stress configurations investigate beyond single scenario usage to the combinations that best stress test the control limits [9].

Phase four concerns governance over data security and privacy. Due to legislation such as the General Data Protection Regulation, as well as sectoral regulation such as banking regulation, privacy-preserving techniques need to be applied to digital twin applications. Data masking techniques can be used to transform sensitive identifiers such as account numbers, counterparty names and transaction amounts. while preserving stress testing relevant features. Synthetic data generation methods can reduce or remove the need to use production data in some test cases. The use of synthetic data avoids the need to expose production data to privacy risks and can provide sufficient statistical fidelity to simulate controls. Digital twin architectures can maintain relevance through access control, encryption, and audit trails.

The fifth phase is model validation and calibration. Before deploying a digital twin in the real environment, the simulated control behavior must be validated against the actual operational behavior for stress testing. Backtesting (running the digital twin model against real historical transaction datasets that include known control outcomes) is the primary empirical validation method, and most sensitive model parameters can be identified through sensitivity analysis [6]. Expert review accounts for knowledge of the institution not captured in the data. Benchmarking against best practices in stress testing validates the method. Continuous validation, periodically revalidating as operational practices mature, ensures that drift does not occur and that the simulation does not become obsolete.

Explicit governance frameworks that define decision rights, escalation paths, remedial action responsibility, and integration points with existing audit and compliance functions must be implemented [12]. In poorly governed organizations, there may be uncertainty about when and how to adapt controls based on digital twin outputs, possibly leading to over-automation of control changes that require human resources to consider, or to overlooking useful insights generated from simulations.

Fig. 2. End-to-end ERP digital twin methodology workflow

5. Resilience Metrics and Organizational Challenges

A properly designed digital twin stress test should have a set of quantifiable resilience metrics that translate the outputs of the stress test simulations into business metrics. For example, the Control Effectiveness Score summarizes the effectiveness of a control across several stress test scenarios based on fraud detection, false positive rates and under-pressure operational behavior. Risk Mitigation Rate is the percentage reduction in the number of control weaknesses identified and remediated using digital twins. This is the analytical ROI generated by stress testing. Operational Efficiency Gain takes into account reduced processing time and queue size and increased throughput resulting from the identified optimization of control workflows that were identified as bottlenecks by the digital twin [13]. Compliance Assurance Level is an indicator of actual regulatory-stressed performance and enables organizations to report and communicate with a confidence level with respect to regulatory reporting and governance.

Fraud detection metrics also receive focus: detection rate, the fraction of fraud scenarios injected by testers that are detected by production controls, is an indication of fraud control efficacy. The false positive rate reflects the cost of controls that are too sensitive and result in good transactions being blocked. Detection time, the time from when fraud occurs to when controls detect it, is useful when detection can allow losses to be reduced [3]. These metrics also allow organizations to determine over many iterations of the simulation whether controls are improving as risk increases and where remediation spending on a control domain has the greatest potential for risk reduction.

Notwithstanding these analysis advantages, the creation of ERP digital twins is inhibited by several major barriers that need to be addressed: The large upfront data infrastructure and simulation software investment and personnel expertise (data engineering, financial process modeling, and digital twin modeling) is a particularly high barrier for organizations with large multi-application data landscapes and complex legacy ERP landscapes [4]. Where organizational change management is necessary, for example, where finance and audit teams are relatively new to simulation-based control validation, the implementation may take longer to allow time for capabilities to be built up.

Organizational resistance is common during the implementation phase. For example, finance and control functions, which are familiar with conventional financial auditing, may resist digital twins as a threat if it is framed as a replacement for human expertise [12]. Governance risk of overconfidence in simulation results should be considered. Organizations that place high trust in their digital twin simulation outputs may deemphasize customary testing approaches, which add unique value by identifying new risks that fall outside of the scope of the digital twin simulation. Regulators place high value on customarily performed attestation audit methodologies. Digital twin approaches have not yet seen sufficient common adoption to act as a replacement for customary audit evidence for regulatory compliance purposes [1].

Due to model inaccuracies, false negatives may exist in the digital twin (genuine weaknesses that the model fails to detect). This results in a false sense of security when the controls are shown to work in the model but not in the environment. It may be necessary to continue investing in model calibration as business processes change in order to maintain model accuracy. Furthermore, organizations may not have the technical ability to properly assess model accuracy [6]. Techniques for protecting privacy by reducing the utility of sensitive financial information may in turn reduce the quality of analysis, leading to a tradeoff [11].

Metric	Definition	Measurement Unit	Primary Beneficiary
Control Effectiveness Score	Aggregated control performance across all stress scenarios	Composite index (0–1 scale)	Internal audit, governance board
Fraud Detection Rate	Percentage of injected fraud scenarios identified by controls	Percentage (%)	Risk and compliance functions
Risk Mitigation Rate	Reduction in identified control weaknesses post-remediation	Percentage (%)	Executive leadership
Operational Efficiency Gain	Improvement in process cycle time and throughput post-optimization	Time units / transaction count	Finance operations
Compliance Assurance Level	Validated control performance across regulatory stress scenarios	Confidence rating (qualitative–quantitative)	Regulatory reporting, external auditors
Detection Latency	Elapsed time between fraud execution and control identification	Time units (hours/minutes)	Fraud prevention teams

Table II Resilience Metrics Framework for Digital Twin-Based Financial Control Stress Testing [13]

Conclusion

Enterprise resource planning digital twins are a structurally sound and operationally feasible generalization of financial control validation that addresses both the limitations of static, point-in-time testing and the concern of testing feasibility by simulating control behavior and resilience under high-impact realistic scenarios. We have proposed a phased approach that can be operationalized from data extraction to process depiction, scenario specification, privacy governance, model validation, and resilience quantification for diverse ERP and regulatory contexts. Digital twin stress testing enables adversarial scenarios to be tested in virtual control environments without operational risk. It converts control validation from a periodic compliance exercise to an evidence-based discipline capable of uncovering latent weaknesses before they lead to material control failures. The metrics of resilience (derived fraud detection rate, risk mitigation rate, compliance assurance level, and operational efficiency gain) provide a structured lexicon for measuring how much a control has improved in a given testing cycle, which enables defensible communications of control effectiveness to governance and regulators. Nevertheless, a realistic implementation needs to acknowledge that there will be some barriers, including capital costs, specialist knowledge, data privacy, organizational culture, and the application of customary audit processes as regulators' attestation platforms. Hybrid schemes that combine simulation-driven coverage and customary audit and organizational processes offer the most credible and viable way forward. Starting with high-risk, high-value financial processes enables stepwise investment, acceleration of learning and demonstration of value to encourage broader adoption. As artificial intelligence and real-time monitoring capabilities develop, the role of digital twins will evolve from periodic stress testing and scenario planning tools to always-on control intelligence platforms. Those organizations that build and invest in foundational capabilities today will be the ones ready to lead next-gen enterprise financial governance.

References

[1] Carlos Bruen, “The System Cannot Fail – Reflections on The Audit Society: Rituals of Verification," 2010. [Online]. Available: https://www.developmenteducationreview.com/issue/issue-11/system-cannot-fail-%E2%80%93-reflections-audit-society-rituals-verification

[2] Joshua Aizenman et al., "Fundamentals and Sovereign Risk of Emerging Markets," National Bureau of Economic Research Working Paper, 2013. [Online]. Available: https://www.nber.org/papers/w18963

[3] Kristina Russo, Financial Statement Fraud: Prevention and Detection, NetSuite. [Online]. Available:

https://www.netsuite.com/portal/resource/articles/accounting/financial-statement-fraud.shtml

[4] Fei Tao et al., "Digital Twin in Industry: State-of-the-Art," IEEE Transactions on Industrial Informatics, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8477101

[5] Edward Glaessgen and David Stargel, "The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles," 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference, 2012. [Online]. Available: https://arc.aiaa.org/doi/10.2514/6.2012-1818

[6] Adil Rasheed et al., "Digital Twin: Values, Challenges and Enablers From a Modeling Perspective," IEEE Access, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8972429

[7] Wil van der Aalst, "Process Mining," Springer Nature Link, 2016. [Online]. Available: https://link.springer.com/book/10.1007/978-3-662-49851-4

[8] Wil van der Aalst et al., "Replaying history on process models for conformance checking and performance analysis," WIREs Data Mining and Knowledge Discovery, 2012. [Online]. Available: https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1045

[9] Miles E.A. Everson et al., "Enterprise Risk Management Integrating with Strategy and Performance." Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017. [Online]. Available: https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[10] Dmitry Ivanov et al., "The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics," International Journal of Production Research, 2019. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/00207543.2018.1488086

[11] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[12] Institute of Internal Auditors (IIA), "The IPPF: The Framework for Internal Audit Effectiveness," 2003. [Online]. Available: https://www.theiia.org/en/standards/international-professional-practices-framework/

[13] M. Hammer and J. Champy, Prologue: Reengineering For The Twenty-First Century. MICHAEL HAMMER & JAMES CHAMPY. [Online]. Available: https://www.harpercollins.com/products/reengineering-the-corporation-michael-hammerjanmes-champy

[14] Robert S. Kaplan and David P. Norton, "Using the Balanced Scorecard as a Strategic Management System," Harvard Business Review, 2007. [Online]. Available: https://hbr.org/1996/01/using-the-balanced-scorecard-as-a-strategic-management-system

[15] Michael Grieves and John Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems," Transdisciplinary Perspectives on Complex Systems, 2016. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-38756-7_4