

Member Communication Experience

The Built Environment Is Missing An Identity Layer

Written by: Trevor Vick, CEO, UMIP, Inc., and Founder, Global Infrastructure Identity Standard (GIIS)

When two steel columns buckled on the 21st floor of the former Pfizer headquarters in Manhattan this July, the building safety industry watched a familiar sequence unfold. Investigators and engineers scrambled to reconstruct what had happened to the 37-story tower, then mid conversion from office space into more than 1,600 apartments.

Reporting from [industry news sources](#) noted that engineers examining the failure were cautioned against assuming the visible damage marked the full extent of the problem, since major structural elements are interconnected and a failure in one area often signals stress elsewhere. Early accounts pointed toward a missing steel reinforcement plate, a detail that should have appeared in the project's engineering plans but never reached the columns themselves, according to engineers cited by [The Real Deal](#).

It would be easy to read this as a documentation failure. That framing undersells what happened. The tower did not lose its documentation. It lost records continuity. Every renovation, every code cycle, every material change was tied to whatever system, contractor, or individual happened to be tracking it at the time. When that link broke, the connective thread of the asset's history broke with it.

The missing layer is not another document repository. It is a persistent identity that connects every record, inspection, permit, renovation, owner, engineer, and software platform to the same physical asset over its entire lifecycle.



DOCUMENTATION ANSWERS THE WRONG QUESTION

This matters well beyond one incident, because even organizations with disciplined document management run into this failure mode. A document repository can answer what records exist on file. It cannot answer what has happened to a specific physical asset across its operating life.

A [recent industry analysis](#) of facility continuity found that as veteran facility managers retire, change jobs, or move on, decades of undocumented building knowledge often leave with them, since that knowledge frequently lives in someone's head rather than in a system. The same analysis cited IFMA projections that more than 45% of facility management professionals worldwide will retire within the next decade, a wave that will test how well institutional memory survives personnel turnover.

That is the same failure described two different ways. Whether the loss shows up as a retiring engineer who carried undocumented knowledge out the door, or a repository that cannot say what a structure can and cannot support after decades of alterations, the cause is identical. Nothing in these systems persistently follows the physical asset itself. The record lives with the software, the vendor, or the employee, never with the infrastructure.

WHAT EMERGENCY RESPONSE ACTUALLY REQUIRES

This is where the stakes sharpen. In a post failure scenario, structural engineers, investigators, and insurers are not simply looking for a folder of drawings. They need a reliable, continuous chain of custody for every material change made to a structure, traceable back to who made it, when, and under what code cycle. A binder handed off at turnover cannot provide it.

The same need extends well beyond structural engineering. Fire departments responding to an active incident, emergency management agencies coordinating a response, FEMA assessing damage after a disaster, insurance adjusters evaluating a claim, building officials issuing permits or certificates of occupancy, and urban search and rescue teams operating inside a compromised structure all depend on the same continuous history of what a building is, what it can support, and what has changed.

What emergency response actually requires is closer to a VIN for a piece of physical infrastructure, a persistent identifier that every contractor, engineer, permitting office, and software platform can reference over decades, regardless of who owns the data or which system created it.

Imagine trying to investigate an aircraft if every maintenance record was stored under a different numbering system every time ownership changed. That would be unacceptable in aviation. Yet it remains normal for buildings.

A SURVEY THAT IS MEASURING SOMETHING DEEPER

Viewed this way, recent [survey findings from ARC Facilities](#) on facility leader confidence are not really measuring documentation quality. They are measuring identity fragmentation. The survey found that many facility leaders

describe only partial confidence in accessing critical building information when it matters most, with one respondent noting plainly that their organization lacks a reliable system, and another describing an ongoing struggle to capture and retain critical knowledge.

Low confidence in complete and accessible records is exactly what should be expected in an industry where every renovation, ownership change, and software migration creates another chance for the connective thread between a physical asset and its history to snap.

THE LAYER THE INDUSTRY NEVER STANDARDIZED

Over the past several decades, the built environment has methodically standardized layer after layer of how infrastructure gets built and managed. CAD standardized design. BIM standardized information. GIS standardized location. IFC standardized interoperability. Digital twins standardized representation. AI is now beginning to standardize intelligence.

What none of those layers ever standardized is identity: a persistent, portable reference that follows a piece of infrastructure across every one of those systems and throughout its lifecycle. Each new platform generation has improved how information about an asset is captured, but none has solved for what happens to that information once the platform, the vendor, or the employee who understood it moves on.

A digital twin cannot remain continuous if the identity of the physical asset it represents is not continuous.

That distinction is worth stating plainly. Interoperability tells systems how to exchange information. Identity tells systems what they are exchanging information about. The industry has spent 50 years perfecting the first problem while leaving the second essentially unaddressed.

A DIFFERENT QUESTION TO ASK

The Pfizer conversion is useful not because documentation failed at a single point, but because continuity failed across an entire history of changes, and continuity ultimately depends on identity.

The more productive question isn't how thoroughly infrastructure gets documented. It's why so little of it carries a persistent identity across ownership changes, renovations, and software migrations. That question spans BIM, GIS, digital twins, AI, insurance, construction, and government alike: every industry exchanges data about buildings without a shared way to identify what it describes.

The built world has standardized nearly every way information is created, exchanged, and analyzed. The next standard will not be another data format. It will be persistent identity. 



About the Author

Trevor Vick is the CEO of [UMIP, Inc.](#) and the founder of the Global Infrastructure Identity Standard (GIIS).

Any views and opinions expressed in this article may or may not reflect the views and opinions of the Construction Management Association of America (CMAA). By publishing this piece, CMAA is not expressing endorsement of the individual, the article, or their association, organization, or company.