인사이트

AI에게 공장 제어를 맡길 수 있을까

신뢰는 어디서 오나

방동걸 (주)웨이스 대표이사

2026년 7월 22일

공장에 AI를 들이는 이야기는 이제 낯설지 않다. 그런데 막상 "AI가 설비를 직접 제어하게 하자"는 대목에서는 대부분 멈칫한다. 이유는 분명하다. 살아 있는 라인에서 잘못된 명령 하나는 불량으로, 정지로, 사고로 이어진다. 대시보드가 틀리면 다시 보면 되지만, 제어가 틀리면 되돌리기 어렵다. VEXPLOR에서 AI 판단을 설비 제어까지 연결해 온 웨이스가 현장에서 늘 받는 질문이다.

그래서 진짜 질문은 "AI가 충분히 똑똑한가"가 아니다. "AI를 믿고 맡길 수 있는가"다. 신뢰는 성능에서 저절로 나오지 않는다. 신뢰는 두 가지에서 온다.



신뢰는 근거에서 옵니다.

01

첫째, AI가 근거 위에서 답할 때

현장에서 범용 AI를 못 믿는 가장 큰 이유는 환각이다. 그럴듯하지만 틀린 답을, 왜 그렇게 답했는지도 모른 채 내놓는다. 생산에 손을 대는 AI가 이러면 곤란하다.

VEXPLOR의 제조 AI는 다르게 동작한다. 모든 답이 공장의 온톨로지에 묶여 있다. 설비, 공정, 품질, 자재가 어떻게 연결되는지를 담은 지식그래프 위에서, 하이브리드 Graph RAG가 답의 근거를 실제 데이터로 되짚는다. 그래서 "이 설비의 이상 원인은 무엇인가"라는 물음에 AI가 답을 낼 때, 그 답이 어느 신호와 어느 이력에서 나왔는지가 함께 보인다.

근거가 보인다는 것은 검증할 수 있다는 뜻이다. 사람이 "왜?"를 물을 수 있고, AI가 그 자리에서 대답할 수 있다. 블랙박스가 아니다. 신뢰의 절반은 여기서 시작된다.

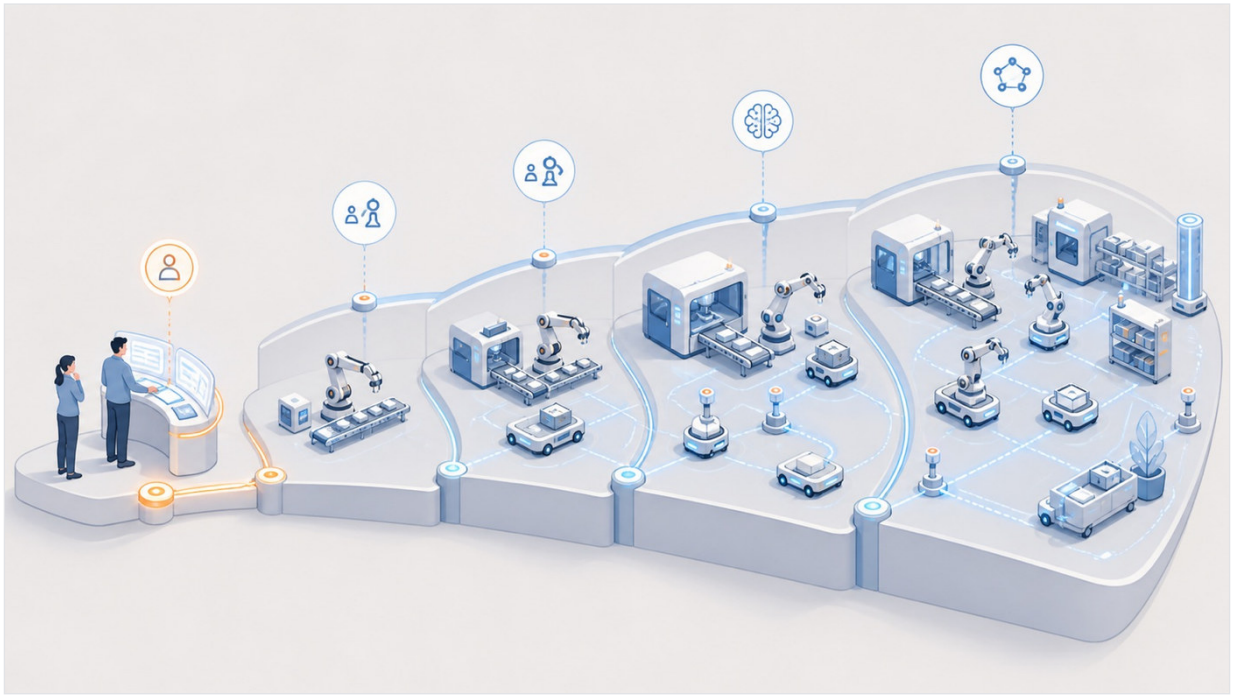
02

둘째, 자율을 단계로 넘길 때

나머지 절반은 제어를 넘기는 방식에 있다. 자율제어를 한 번에 전부 맡기는 것은 누구에게도 부담이다. VEXPLOR의 제어 커널은 자율을 등급으로 나눠 넘긴다. AAF라 부르는 이 단계는 L0에서 L4까지, 사람이 확인한 만큼만 AI에게 권한을 넘긴다.

여기에 한 겹이 더 있다. 위험한 명령은 실행되기 전에 막는다. SHACL 규칙이 명령을 실행 직전에 검사해, 안전 범위를 벗어나는 동작은 애초에 나가지 못하게 한다. AI가 아무리 자신 있게 판단해도, 검증되지 않은 위험한 제어는 라인에 닿지 않는다.

그래서 공장은 자기 속도로 자율화를 넓혀 간다. 처음에는 AI가 감지하고 제안만 하게 두고, 신뢰가 쌓이면 한 단계씩 권한을 올린다. 사람은 언제든 지켜보고, 확인하고, 되돌릴 수 있다. 자율은 사람을 밀어내는 것이 아니라, 사람이 감당하던 판단을 검증된 만큼 이어받는 것이다.



자율은 한 번에 넘기지 않고 단계로 넘깁니다.

03

신뢰 위에 자율이 선다

근거 있는 AI는 "왜 그렇게 판단했는지"를 보여 주고, 단계형 자율제어는 "얼마나 맡길지"를 사람이 정하게 한다. 이 둘이 함께여야 살아 있는 현장에서 AI에게 제어를 맡길 수 있다. 실제로 이 방식은 이미 20곳이 넘는 제조 현장에서 돌고 있고, 자율형공장 실증(스피폭스)에서 검증되고 있다.

공장 자동화의 다음 단계는 더 똑똑한 AI가 아니라, 믿고 맡길 수 있는 AI다. VEXPLOR는 그 신뢰를 근거와 단계로 설계한, 제조 AI 운영체제다.

WACE(웨이스)는 공장이 스스로 판단하고 멈추지 않게 하는 제조 AI 운영체제 VEXPLOR를 만드는 회사다.

원문 blog.vexplor.com/post/trusting-ai-with-factory-control
발행 2026년 7월 22일 · 방동걸 (주)웨이스 대표이사

회사 주식회사 웨이스 (WACE Inc.) · 대표이사 방동걸 · 사업자등록번호 439-87-02852
주소 (18462) 경기 화성시 동탄영천로 150, 에이동(A동) 1702-1708호 (영천동, 실리콘앨리동탄)
연락처 전화 070-4730-0629 · contact@wace.me
홈페이지 wace.me · linkedin.com/company/wace-inc

원문 홈페이지 링크드인