

AI/ML

양자컴퓨터 복구 성공률 58%를 AI가 끌어올렸습니다

장비를 맡기는 인터페이스는 어떻게 짜는가

방동걸 (주)웨이스 대표이사

2026년 8월 31일

양자컴퓨터의 레이저 주파수 잠금이 풀리면 다시 잡아야 합니다. 벤더 스크립트의 복구 성공률은 58%, 한번에 150초가 걸렸습니다. AI 에이전트가 밤새 그 절차를 스스로 고쳐 쓴 결과, 아침에는 6초에 96%가 됐습니다. 그렇게 완성된 스크립트를 같은 교란 세트로 다시 돌리자 700회 중 695회, 99.3%였습니다. 이 마지막 측정에는 에이전트가 개입하지 않았습니다. VEXPLOR로 공장 설비를 AI와 연결하는 웨이스가 이 결과를 제조 현장 기준으로 다시 읽었습니다.

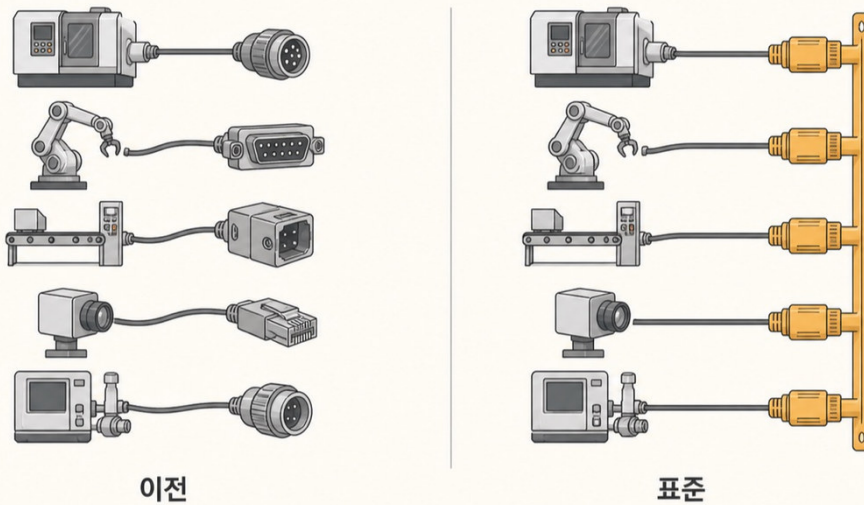
엔트로픽이 2026년 8월 27일 공개한 모델 하드웨어 표준(MHS, Model Hardware Standard) 연구 프리뷰에 실린 QuEra Computing의 수치입니다. 발표문에는 이런 수치가 여섯 현장 분량으로 실려 있습니다. 이 글은 그 발표를 "AI에게 물리 장비를 맡기는 인터페이스를 어떻게 짜는가"라는 설계 문제로 뜯어 읽은 기록입니다. 수치는 전부 공식 발표문 기준입니다.

1. 문제: 장비마다 말이 다르다

실험실이든 공장이든 사정은 같습니다. 현미경은 현미경대로, 액체 핸들러는 핸들러대로, 로봇팔은 로봇팔대로 제조사가 정한 인터페이스로만 말합니다. HHMI Janelia의 2광자 현미경 시스템은 공용 인터페이스 없이 벤더 프로그램 7종으로 갈려 있었고, 제어 언어도 검출기는 MATLAB, 카메라는 Python, 전기생리는 C#으로 흩어져 있었습니다. 실험 하나를 시작하려면 프로그램 7개를 정해진 순서대로 띄워야 했고, 순서를 틀리면 그날 세션을 통째로 날렸습니다. 장비를 하나 추가하려면 며칠, 시스템을 새로 통합하려면 몇 주에서 몇 달이 듭니다. 그리고 그 통합은 장비를 바꿀 때마다 다시 해야 하는 일이라, 한 번 치르고 끝나는 비용이 아닙니다.

MHS는 이 통합 작업을 시간·분 단위로 줄이는 것을 목표로 합니다. 실제로 카네기멜런 연구팀은 액체 핸들러·플레이트 리더·로봇팔·카메라를 컴퓨터 3대에 걸쳐 잇는 데 8시간이 들었습니다. 벤더 구축 견적은 몇 주였습니다.

장비마다 말이 다르다



장비마다 다른 커넥터가 하나의 표준 레일로 모이는 그림

장비마다 다른 인터페이스를 쓰던 것이 하나의 표준 연결로 바뀐다. MHS가 겨냥하는 지점이다.

2. 설계 선택 셋

발표문에서 읽히는 설계 선택은 세 가지입니다.

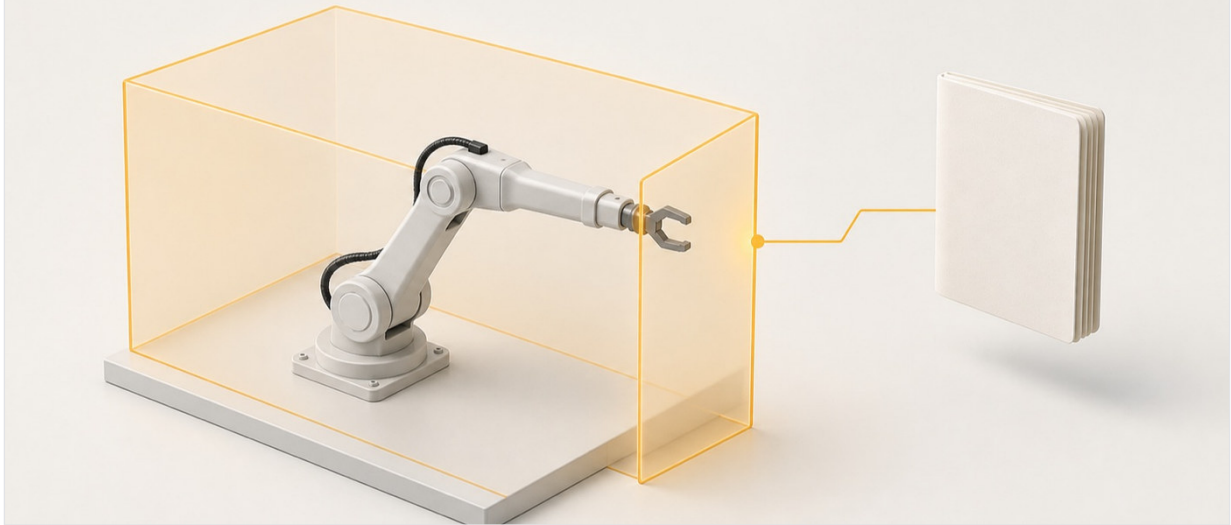
첫째, 프리미티브를 둘로 줄였습니다. 모든 장비 기능을 read(온도를 읽는다)와 write(온도를 설정한다)로 표현합니다. 장비가 수백 종이어도 동사는 두 개뿐이니, 에이전트는 장비별 매뉴얼이 아니라 하나의 문법만 배우면 됩니다. 장비 자동 발견까지 없어서 장비별 "번역기" 프로그램을 없앴습니다.

둘째, 장비 설명서를 자연어 태그로 만들었습니다. 로봇팔의 무게, 측정 가능 범위, 조정 가능한 파라미터, 그리고 안전 제한값을 자연어 메타데이터로 달아 두면 참조 파일이 자동 생성되고, 에이전트는 처음 보는 장비도 그 파일을 읽고 다룹니다. 사람용 매뉴얼과 기계용 프로토콜 사이에 "AI가 읽는 문서"라는 세 번째 층을 만든 것인데, 이 층이 MHS의 실질입니다. 프로토콜 통일은 이전에도 여럿 있었지만, 장비의 물리 특성과 안전 조건을 모델이 이해하는 형식으로 실어 나른다는 점이 이전 표준들과 갈리는 지점입니다.

덧붙여, 제어 경로를 3가지로 열어 뒀습니다. MCP 서버로 붙을 수도 있고, 커맨드라인으로 칠 수도 있고, 장시간 도는 작업은 코드 파일에서 드라이버 명령을 엮을 수도 있습니다. 모델에 종속되지 않는다는 점도 명시돼 있어서, 특정 회사의 에이전트가 아니라 표준 프로토콜을 쓰는 어떤 하니스든 접근할 수 있습니다. 표준을 자기 제품에 묶지 않겠다는 선언인데, 이게 지켜지는지가 이 표준의 수명을 정할 겁니다.

셋째, 안전 제한을 사양 안에 넣었습니다. 레이저 출력 상한 같은 제한을 에이전트의 판단이 아니라 장비 기술 계층에서 강제합니다. "모델이 알아서 조심한다"가 아니라 "장비 쪽에서 넘지 못하게 만든다"입니다. 물리 세계에서는 이 순서가 맞습니다. 잘못된 API 호출은 롤백하면 되지만 잘못된 레이저 출력은 롤백이 없기 때문입니다.

안전은 사양에 넣는다



로봇팔이 사양서와 연결된 안전 경계에 막히는 그림

안전 제한을 모델의 판단이 아니라 장비 기술 계층에 두는 구조. 잘못된 설비 동작은 되돌릴 수 없기 때문이다.

3. 수치가 말해주는 것

여섯 파일럿의 수치를 나란히 놓으면 패턴이 보입니다.

현장	과제	결과
QuEra	레이저 잠금 복구	58% → 96%(하룻밤 개발 실행), 150초 → 6초
QuEra	완성 스크립트 블라인드 테스트	700회 중 695회 = 99.3%. 어려운 교란 1014초, 쉬운 교란 0.95.4초 (사람은 5~10분)
QuEra	PID 파라미터 튜닝	잔여 오차 15.7mV → 1.55mV (약 10배)
카네기멜런	용량-반응 실험	속도 3배, 통합 8시간

현장	과제	결과
UW 단백질설계 랩	장비 6종 통합	1주 미만 (종전 수 주~수 년)
Janelia	카메라 추가	수 일 → 수 분

반복 조정형 과제 — 잠금 복구, PID 튜닝, 농도 범위 조정 — 에서 AI가 사람과 벤더 스크립트를 넘었습니다. QuEra의 PID 튜닝은 Claude가 16시간 동안 363회 실험을 스스로 돌려 얻은 값이고, 19시간 연속 가동에서 잠금 이탈이 0회였습니다. 전문가 튜닝은 시간당 1.6회 이탈했습니다. 지루한 반복 실험을 무한정 돌릴 수 있다는 것 자체가 능력이 되는 영역입니다.

여기서 눈여겨볼 것이 하나 더 있습니다. QuEra의 최종 산출물은 에이전트가 아니라 **에이전트가 써낸 확정적이고 전부 들여다볼 수 있는 스크립트**였습니다. 99.3%는 그 스크립트를 에이전트 없이 돌려 켤 값입니다. AI가 현장에 남긴 것이 판단 주체가 아니라 검증 가능한 산출물이었다는 뜻인데, 물리 장비를 다루는 영역에서는 이 형태가 더 오래갈 가능성이 큼니다.

수치 하나만 더 보겠습니다. Tetsuwan Scientific은 액체 분주 9,143회를 테스트해 전송 유형 300종·측정 조건 1,508개를 모았고, 그렇게 다듬은 모델이 **제조사가 제공한 사양보다 12% 정확**했습니다(부호검정 $p \approx 0.001$). 장비를 만든 회사가 문서에 적어 둔 값보다, 그 장비를 수천 번 돌려 본 데이터가 더 정확했다는 뜻입니다.

이게 이 표준이 여는 진짜 문일지 모릅니다. 지금까지 장비의 특성은 매뉴얼에 적힌 값이었는데, 장비가 표준 인터페이스로 열리면 그 값은 **각 현장에서 측정되는 값**이 됩니다. 카네기멜런 팀이 플레이트 누락·회전·연결 끊김 같은 인위 장애 6종을 만들어 전부 차단되는지 확인한 것도 같은 성격입니다. 표준이 통합만 쉽게 만드는 게 아니라, 검증을 반복 가능하게 만듭니다.

4. 함정 셋 — 발표문이 스스로 적어둔 것

성과 수치보다 더 눈여겨볼 것은 발표문에 남아 있는 한계 서술입니다.

함정 1. 물리 직관은 아직 없습니다. Genentech 파일럿에서 액체 분주 속도를 최적화하던 에이전트는 거품이 생기는 물리적 원인을 이해하지 못해, 사람이 "액체를 더 부드럽게 다루는 파라미터 쪽으로" 유도해야 했습니다. 엔트로픽 스스로 "Claude did not yet understand the underlying physics of the failure"라고 적었습니다. 데이터에 없는 물리는 모델에도 없습니다. 그 물리를 아는 것은 여전히 그 현장의 사람입니다.

함정 2. 파일럿 여섯 곳 중 다섯이 실험실입니다. 생명과학 넷, 양자 하나. 제조 현장은 발표 문구("advanced manufacturing")에만 있고 정량 사례가 없습니다. 실험실은 장비가 정형적이고 실패 비용이 시약 한

판이지만, 제조 라인은 이기종 설비 수백 대가 몰려 돌고 실패 비용이 라인 정지입니다. 실험실에서 검증된 수치를 제조로 그대로 가져와 말하면 과장이 됩니다.

함정 3. 99.3%의 나머지 0.7%가 물리 세계에 남습니다. 소프트웨어라면 700번 중 5번의 실패는 재시도로 지워집니다. 물리 세계에서는 그 5번이 어떤 상태로 끝났는지 — 안전하게 멈췄는지, 이상한 상태로 남았는지 — 가 전부입니다. 그래서 1차 성공률만큼이나 "실패가 어떤 모양으로 실패하는가"를 설계해야 하고, MHS가 안전 제한을 사양에 내장한 이유도 여기에 있습니다. 오픈소스 공개 시점을 안전성 평가 뒤로 묶어 둔 것도 같은 맥락입니다.

5. 통합이 흔해지면 무엇이 남는가

MHS는 지금 연구 프리뷰이고, 사양과 코드는 미공개이며, 오픈소스 시점도 미정입니다. 그러나 방향은 분명합니다. AWS·두산로보틱스·유니버설로봇·Tecan·QIAGEN·허깅페이스가 파트너 명단에 있고, 표준이 풀리면 "장비를 잇는 일" 자체는 빠르게 흔한 기술이 될 겁니다.

이 표준이 오픈소스로 풀린 다음의 그림을 그려 보면 이렇습니다. 장비 제조사는 자기 장비의 MHS 드라이버를 함께 내놓게 되고, 통합 업체가 몇 주씩 들여 만들던 연결 코드는 상당 부분 사라집니다. 지금 그 연결 코드를 자산이라 부르고 있는 팀이라면, 자산의 수명이 짧아지는 국면입니다.

그때 남는 것은 두 가지라고 봅니다. 하나는 함정 1의 물리 직관 — 그 현장의 공정을 아는 도메인 지식입니다. 또 하나는 함정 3의 검증 — AI의 판단이 장비로 나가기 전에 통과해야 하는 확인 계층입니다. 통합 계층을 직접 짜고 있는 팀이라면, 지금 만드는 코드를 두 칸으로 나눠 보는 것이 이 발표를 읽는 실용적인 방법일 겁니다. 한 칸은 "장비와 말을 트는 코드" — 표준이 대체할 쪽입니다. 다른 칸은 "그 장비가 이 공정에서 어떻게 동작해야 하는지 아는 코드" — 표준이 대체하지 못하는 쪽이고, 그건 어차피 그 현장에서만 자랍니다.

두 칸의 비율이 지금 어떻게 되는지가, 이 표준이 풀렸을 때 무엇이 남는지를 그대로 말해 줄 겁니다.

참고: [Previewing the Model Hardware Standard \(Anthropic, 2026-08-27\)](#)

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



원문	blog.vexplor.com/post/how-mhs-lets-ai-touch-hardware
발행	2026년 8월 31일 · 방동걸 (주)웨이스 대표이사
회사	주식회사 웨이스 (WACE Inc.) · 대표이사 방동걸 · 사업자등록번호 439-87-02852
주소	(18462) 경기 화성시 동탄구 동탄영천로 150, 에이동(A동) 1332·1333·1334·1335호 (영천동, 실리콘엘리동탄)
연락처	전화 070-4730-0629 · contact@wace.me
홈페이지	wace.me · linkedin.com/company/wace-inc



원문



홈페이지



링크드인