2026 년 7 월까지의 공개 기술 변화로 읽는

2026 하반기 Physical AI 동향

모델이 몸을 얻은 뒤, 무엇이 달라지는가

인지하고, 기억하고, 계획하고, 움직인 뒤 다시 확인하는 시스템.
이 책은 Physical AI 를 “큰 모델 하나” 가 아니라
결과를 확인하고 실패를 복구하는 폐루프로 읽는 해설서다.

2026 년 하반기 전망판 • 다섯 변곡점 심화 분석 • 2026 년 7 월 26 일 기준

이 책을 펼치기 전에

로봇이 컵을 정확히 알아봤다고 해봅시다. 지시도 알아들었고, 팔도 움직였습니다. 그런데 컵을 떨어뜨렸다면 우리는 그 로봇의 인식이 성공했다고 말해야 할까요? 디지털 AI 에서는 좋은 답을 내놓는 일이 결과의 끝인 경우가 많습니다. Physical AI 에서는 출력이 환경을 바꿉니다. 잘못된 답은 틀린 문장이 아니라 충돌, 파손, 정지 시간, 사람의 개입으로 이어집니다.

그래서 이 책은 모델의 이름이나 기록을 줄 세우지 않습니다. 대신 로봇 한 대를 현장에 투입한다는 사고실험을 따라갑니다. 명령을 알아듣는 일에서 시작해 공간을 재고, 접촉을 느끼고, 긴 작업을 기억하고, 미래를 상상하고, 실패를 복구하며, 여러 로봇에 업데이트를 배포하는 데까지 차례로 걸어갑니다.

전망의 범위와 판정 기준

여기서 먼저 중요한 경계를 하나 그어둡시다. 이 책은 2026 년 7 월 26 일까지 공개적으로 확인할 수 있는 기술 변화에 기초해, 하반기에 무엇을 관찰해야 하는지를 해설합니다. 하반기 전체를 이미 일어난 사실처럼 서술하지 않습니다. "확산될 것이다" 라고 단정하기보다, 어떤 조건이 충족되면 그 방향이 강해지는지와 어떤 숫자가 전망을 뒤집는지를 함께 적습니다.

이 책의 중심 명제는 간단합니다.

> *2026* 년의 중요한 변화는 더 큰 모델의 등장에 그치지 않고, 인지–기억–계획–행동–검증–복구가 하나의 실행 루프로 연결되기 시작했다는 점이다.

좋은 엔진 하나가 좋은 항공기를 만들지 못합니다. 엔진, 조종계통, 항법, 경보, 정비 체계가 연결되어야 비행이 됩니다. Physical AI 도 이제 "엔진 시연" 에서 "항

공기 조립” 으로 넘어가는 중입니다. 이 비유를 기억하면 뒤에 나오는 VLA, 월드모델, 메모리, 3D 표현, 촉각, 런타임 검증 같은 용어들이 각자 어디에 놓이는지 훨씬 잘 보일 것입니다.

읽는 법

각 상자의 제목은 해당 내용의 핵심 주장을 직접 제시합니다. 본문은 기술 변화의 원인과 구조를 설명하고, 사례와 현장 지표는 그 주장을 실제 시스템에서 확인하는 방법을 보여줍니다.

공개 자료의 근거 범위

공개된 기술 보고서와 프로젝트 페이지는 최신 방향을 읽는 데 유용하지만, 독립적인 재현을 모두 보장하지는 않습니다. 기업 발표의 수치는 해당 팀의 조건에서 보고된 결과로 읽고, 분야 전체의 보편적 성능으로 일반화하지 않습니다. 또한 산업용 로봇 안전 표준이나 AI 규정의 적용 범위는 제품과 용도에 따라 다르므로, 특정 문서가 모든 로봇을 자동으로 규율한다고 해석해서는 안 됩니다.

Contents

이 책을 펼치기 전에 iii

1 왜 지금 Physical AI 인가 1

1.1 지능이 화면 밖으로 나오는 순간 1

1.2 2026 년에 동시에 도착한 다섯 변화 2

1.3 시간축으로 보는 전환 3

1.4 세 가지 역설 4

1.4.1 범용성이 커질수록 검증 범위도 커진다 4

1.4.2 사실적인 영상도 물리 오류를 감출 수 있다 4

1.4.3 계속 학습하면 시스템은 승인 당시의 상태와 달라진다 . . . 4

2 명령을 로봇 행동으로 바꾸는 법 6

2.1 VLA 의 경제적 가치는 재사용성에 있다 6

2.2 느린 뇌와 빠른 손 7

2.3 연속 행동과 확산·플로 8

2.4 추가 학습 없이 더 잘하게 만드는 방법 8

2.5 실전 정책의 기본 조건: 페루프 평가 9

3 로봇은 무엇을 보고 있다고 믿는가 11

3.1 픽셀에서 행동 가능한 공간으로 11

3.2 왜 3D·BEV·LiDAR 가 다시 중요한가 12

3.2.1 Occupancy: 물체 목록보다 자유 공간 12
3.3 SLAM 의 지도는 공간 기억으로 확장된다 13
3.3.1 Gaussian splatting 의 위치 13
3.4 시각만으로는 접촉을 알 수 없다 14
3.5 센서를 더 달면 정말 더 똑똑해지는가 14

4 기억하고 상상하고 계획하는 로봇 16
4.1 긴 입력창과 작업 기억은 다르다 16
4.2 월드모델은 행동 선택을 위한 예측 도구다 17
4.3 추론의 문장과 행동은 일치하는가 18
4.4 과업 계획과 동작 계획의 재결합 18
4.5 장기 작업은 신뢰성의 곱셈이다 18
4.6 복구 가능한 계획 19

5 몸이 달라지면 지능도 달라진다 21
5.1 조작은 종합시험이다 21
5.1.1 양손과 정교 조작 21
5.2 휴머노이드와 다족 보행 22
5.3 항법은 이동이 아니라 임무 수행이다 22
5.4 자율주행이 먼저 보여준 것 23
5.5 UAV 에 한꺼번에 드러나는 제약 23
5.6 기체 간 전이: 무엇을 옮길 것인가 24

6 데이터는 쌓는 것이 아니라 운영하는 것이다 26
6.1 실세계 데이터가 비싼 이유 26
6.2 인간 영상, 시연, 선호는 서로 다르다 27

6.3 생성·시뮬레이션은 통제된 실험 장치다 27
6.4 무학습 일반화라는 말을 분해해서 보자 28
6.5 현장 적응은 작고 되돌릴 수 있어야 한다 29

7 한 대의 로봇에서 하나의 조직으로 31
7.1 협력은 통신보다 역할 설계다 31
7.2 공유해야 할 것과 공유하지 말아야 할 것 32
7.3 중앙과 분산 사이 32
7.4 좋은 업데이트도 대규모 실패가 될 수 있다 33

8 데모를 제품으로 바꾸는 법 34
8.1 평균 성공률이 숨기는 것 34
8.2 강건성과 일반화는 무너지는 조건으로 설명하라 35
8.3 안전은 실행 보증 계층이다 35
8.4 효율은 안전과 경제성의 문제다 36
8.5 실패를 다루는 네 단계 36
8.6 평가자가 독립적이어야 하는 이유 37

9 2026 년 하반기에서 2030 년까지 38
9.1 하반기: 통합을 증명하는 시간 38
9.2 2027–2028: 모듈화와 검증 39
9.3 2029–2030: 운영체제형 계층 39
9.4 이 전망을 뒤집을 신호 40
9.5 연구자와 조직을 위한 질문 41
9.5.1 연구자에게 41
9.5.2 제품 책임자에게 41

9.5.3 회사 운영자에게 41

에필로그: 로봇에게 책임을 묻다 **43**

다섯 변곡점의 심화 분석 **46**

심화 분석: 다섯 변곡점과 2026 년 중순 **46**

심화 분석 01: 일반화의 단위가 커졌다 47

심화 분석 02: 월드모델이 실행 구조에 들어왔다 49

심화 분석 03: 메모리·계층·검증기의 분리 51

심화 분석 04: 실로봇 평가가 데모의 간극을 드러냈다 54

심화 분석 05: 표준·규제가 안전성 입증을 설계 요구로 만들었다 56

심화 분석: 다섯 변곡점을 하나의 구조로 합치기 59

핵심 개념 지도 **62**

핵심 개념: 정책과 시간척도 **63**

핵심 개념: 세계 상태와 감각 **65**

핵심 개념: 기억·추론·미래 **67**

핵심 개념: 몸과 응용 **69**

핵심 개념: 신뢰성·데이터·운영 **71**

더 읽을 거리 **73**

1

왜 지금 Physical AI 인가

이 장의 한 문장

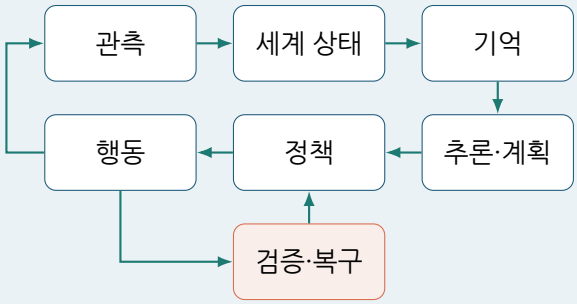
질문이 “로봇이 할 수 있는가” 에서 “반복해서 맡겨도 되는가” 로 바뀌고 있다.

1.1 지능이 화면 밖으로 나오는 순간

디지털 모델은 틀리면 다시 생성할 수 있습니다. 로봇은 한 번의 잘못된 행동으로 대상의 위치를 바꾸고, 다음 입력까지 바꿉니다. 바로 이 점 때문에 Physical AI 는 **폐루프 시스템으로 설계하고 평가해야 합니다**. 관측이 행동을 만들고, 행동이 세계를 바꾸며, 바뀐 세계가 다음 관측이 됩니다.

그동안 로봇 연구의 많은 성과는 각각의 부품에서 나왔습니다. 카메라는 물체를 더 잘 찾았고, 언어 모델은 복잡한 지시를 해석했으며, 정책은 시연된 동작을 더 자연스럽게 재현했습니다. 문제는 부품의 성능을 더한다고 시스템의 신뢰성이 자동으로 생기지 않는다는 데 있습니다. 인식이 맞아도 좌표가 틀릴 수 있고, 계획이 맞아도 모터 명령이 늦을 수 있으며, 한 단계의 작은 오차가 긴 작업에서 누적될 수 있습니다.

폐루프를 이루는 일곱 역할



모델 하나가 이 역할을 모두 맡을 필요는 없다. 중요한 것은 역할 사이의 상태와 책임이 끊기지 않는 것이다.

1.2 2026 년에 동시에 도착한 다섯 변화

첫째, 시각–언어–행동을 잇는 범용 정책이 단순한 새 물체 인식을 넘어 **새 과업의 조합**과 **다른 기체로의 전이**를 겨냥하기 시작했습니다. 범용성의 가치는 "말을 알아듣는다" 는 데서 끝나지 않습니다. 새 작업마다 정책을 처음부터 다시 만드는 비용을 줄이는 데 있습니다.

둘째, 월드모델이 그럴듯한 영상을 만드는 생성기에서 행동의 결과를 미리 시험하는 장치로 확장되고 있습니다. 카메라 영상뿐 아니라 라이다 같은 센서 출력을 함께 생성하고, 후보 행동에 따른 미래를 비교하며, 희귀 상황을 통제된 방식으로 재현하려는 시도가 연결됩니다.

셋째, 메모리, 계층적 계획, 빠른 제어기, 런타임 검증기가 각자의 역할을 가진 부품으로 드러났습니다. 긴 입력창 하나로 모든 이력을 밀어 넣는 대신, 어떤 상태를 보존하고 어떤 판단을 느리게 하며 어떤 반응을 빠르게 해야 하는지가 설계 문제로 올라왔습니다.

넷째, 실제 로봇과 장기 작업을 이용한 평가가 선별된 짧은 데모와 평균 성공률의 한계를 더 분명히 보여주고 있습니다. 한 번의 성공보다 여러 환경에서의 반복 가능성, 사람 개입, 부분 성공, 복구 시간이 중요해졌습니다.

다섯째, 안전 표준과 규제 적용 일정이 인간 감독, 로그, 강건성, 사후 모니터링을 현실적인 설계 제약으로 끌어올리고 있습니다. 이것이 연구의 유일한 원인은 아니지만, 제품을 만드는 조직에는 모델 선택과 시스템 구조를 바꾸는 압력으로 작동합니다.

모델 밖으로 이동한 병목

이 다섯 변화를 하나의 문장으로 줄이면, **모델의 성능과 적용 범위가 넓어지면서 모델 바깥의 병목이 전면에 드러나기 시작했다**는 것입니다. 추론 지연, 기억 오염, 센서 보정, 실패 복구, 승인된 업데이트 범위는 예전에도 있었지만, 범용 정책이 여러 작업에 적용되기 시작하면서 더 이상 주변 문제로 남지 않게 됐습니다.

1.3 시간축으로 보는 전환

시기	중심 변화
2023–2024	대규모 로봇 데이터 혼합, 생성형 연속 행동, 서로 다른 기체의 경험을 함께 학습하는 토대가 마련됐다.
2025	언어와 행동의 공통 인터페이스, 행동 압축, 엣지 실행, 실시간 행동 묶음, 고수준–저수준 정책 분리가 구체화됐다.
2026 년 상반기	메모리, 월드모델, 런타임 검증, 현장 보정, 다중 센서 생성이 같은 실행 루프 안으로 들어오는 공개 사례가 늘었다.
2026 년 하반기	통합된 스택이 실제로 오래 작동하는지, 실패를 얼마나 빨리 알아채고 복구하는지, 현장 비용을 줄이는지가 관찰 포인트다.
2027 년 이후	모델 크기보다 가동률, 사람 개입, 복구, 데이터 순환, 안전 근거, 롤백이 차이를 만들 가능성이 크다.

1.4 세 가지 역설

1.4.1 범용성이 커질수록 검증 범위도 커진다

열 가지 작업만 하는 로봇보다 백 가지 작업을 하는 로봇이 매력적입니다. 그러나 가능한 상태와 실패 경로도 함께 늘어납니다. 앞으로 "범용" 이라는 주장은 가능한 작업의 수만 말해서는 부족합니다. 무엇을 거절하는지, 어느 불확실성에서 사람에게 넘기는지, 어떤 기체와 환경까지 검증했는지를 함께 제시해야 합니다.

1.4.2 사실적인 영상도 물리 오류를 감출 수 있다

월드모델이 만든 미래 장면이 눈으로 보기에 훌륭해도 접촉력, 마찰, 충돌 가능성, 인과 관계가 맞는다는 보장은 없습니다. 사람은 사실적인 장면을 쉽게 믿습니다. 그래서 생성 품질의 향상은 오히려 검증 기준을 더 엄격하게 만들어야 합니다.

1.4.3 계속 학습하면 시스템은 승인 당시의 상태와 달라진다

현장에서 배운 로봇은 같은 실수를 줄일 수 있습니다. 동시에 어제 승인한 행동과 오늘의 행동이 달라집니다. 지속 학습을 제품에 넣으려면 업데이트 범위를 제한하고, 그림자 평가를 거쳐 일부 기체에 단계적으로 배포하며, 즉시 되돌릴 수 있는 버전 관리 체계를 갖춰야 합니다.

2026 년 하반기에 볼 숫자

전체 작업 성공률	짧은 하위 동작이 아니라 시작부터 종료까지 완수한 비율
사람 개입률	시간당 또는 작업당 사람이 멈추거나 수정한 횟수
복구 성공률	실패를 감지한 뒤 초기화 없이 국소적으로 정상 상태로 돌아온 비율
꼬리 지연	평균이 아니라 95·99 백분위수에서 측정한 인지–행동 지연
가동률과 처리량	하루 동안 실제 일한 시간과 단위 시간당 완료 작업
업데이트 회귀	새 버전이 기존에 되던 작업을 망가뜨린 비율

2

명령을 로봇 행동으로 바꾸는 법

이 장의 한 문장

범용 정책의 역할은 모든 모터 명령을 직접 생성하는 것이 아니라, 상대적으로 느린 고수준 판단과 빠른 물리 반응을 안정적으로 연결하는 것이다.

2.1 VLA 의 경제적 가치는 재사용성에 있다

Vision-Language-Action, 줄여서 VLA 는 시각과 언어를 행동에 연결하는 정책을 뜻합니다. 흔히 "말로 시키면 움직이는 로봇" 으로 소개되지만, 산업적 핵심은 자연어 인터페이스보다 **정책 자산의 재사용**입니다. 물체, 작업, 장면, 기체가 바뀔 때마다 데이터 수집과 정책 개발을 처음부터 반복하지 않을 수 있다면 개발 비용 구조가 달라집니다.

다만 범용 정책이 곧 범용 제품은 아닙니다. 언어에 기반한 고수준 판단은 상대적으로 느리고 추상적입니다. 모터 제어는 빠르고 수치적입니다. "컵을 조심히 잡아라" 라는 지시를 이해하는 판단은 초 단위로 갱신되어도 되지만, 접촉 직전의 힘과 위치는 밀리초 단위로 반응해야 합니다. 큰 모델 하나가 두 시간척도를 모두 맡으면 지연이 커지고 동작을 검증하기도 어려워질 수 있습니다.

범용성보다 재사용성

여기서 중요한 단어는 **범용**보다 **재사용**입니다. 모든 상황에서 잘하는 하나의 정책을 상상하면 곧바로 과장이 됩니다. 더 현실적인 그림은 공통 지식과 언어 인터페이스를 재사용하되, 기체별 제어기와 안전 계층이 그것을 제한하는 구조입니다.

2.2 느린 뇌와 빠른 손

Physical AI 의 정책 스택은 서로 다른 시간척도로 나누어 보는 것이 좋습니다.

계층	대표 주기	맡을 일
임무·추론	수 초 이상	목표 해석, 제약 확인, 도구와 하위 작업 선택
기술·행동 묶음	수백 ms–수 초	잡기, 놓기, 이동 같은 동작의 생성과 전환
반사·서보 제어	수 ms–수 십 ms	접촉, 균형, 미끄러짐, 충돌 여유의 즉각 보정
안전 감시	사건 기반·상시	위험 후보 차단, 속도 제한, 정지, 사람 호출

이 계층을 회사에 빗대면, 임무 정책은 경영진, 기술 선택기는 현장 반장, 저수준 제어기는 숙련 작업자에 가깝습니다. 경영진이 모터 전류까지 매번 결정해서는 안 되고, 작업자가 회사의 장기 목표를 매 순간 다시 해석해서도 안 됩니다. 좋은 구조는 각 층이 무엇을 결정하고 무엇을 보고해야 하는지 명확합니다.

2.3 연속 행동과 확산·플로

로봇의 연속 행동에는 정답이 하나가 아닌 경우가 많습니다. 컵을 오른쪽으로 돌아 잡아도 되고 왼쪽으로 돌아 잡아도 됩니다. 단순 회귀는 서로 다른 성공 경로를 평균내어 오히려 장애물의 가운데로 향하는 이상한 행동을 만들 수 있습니다. 확산·플로 계열의 정책은 여러 가능한 행동 분포를 보존하는 데 강점이 있습니다.

그러나 생성 과정이 반복적이면 추론 시간이 길어집니다. 샘플 수를 줄이면 빨라지지만 행동 다양성과 안정성이 손상될 수 있습니다. 행동을 긴 묶음으로 한 번에 만들면 효율적이지만, 실행 중 환경이 바뀌었을 때 오래된 계획을 계속 수행할 위험이 생깁니다.

행동 묶음의 길이가 만드는 절충

$$\text{긴 행동 묶음} \Longrightarrow \begin{cases} \text{추론 호출 감소, 움직임의 부드러움 증가} \\ \text{환경 변화에 대한 반응성 감소} \end{cases}$$

$$\text{짧은 행동 묶음} \Longrightarrow \begin{cases} \text{재관측과 보정 기회 증가} \\ \text{계산량, 지연 변동, 경계 진동 증가} \end{cases}$$

해법은 하나가 아닙니다. 실행과 추론을 비동기로 돌리거나, 위험이 낮을 때는 긴 묶음을 쓰고 접촉이나 사람이 가까운 순간에는 짧게 바꾸거나, 빠른 작은 정책이 큰 모델의 출력을 보정할 수 있습니다. 중요한 것은 평균 지연 하나가 아니라 **지연의 꼬리값**과 행동 경계에서의 불연속을 함께 재는 일입니다.

2.4 추가 학습 없이 더 잘하게 만드는 방법

모든 현장과 작업마다 가중치를 다시 학습하면 버전 관리와 회귀 시험 비용이 커집니다. 그래서 가중치를 고정한 모델 위에 검색, 메모리, 도구 호출, 후보 샘플링, 검증기를 붙여 추론 시점에 개선하는 방식이 매력적입니다. “학습이 없다” 는 말은

비용이 없다는 뜻이 아닙니다. 계산량과 검색 지연이 늘고, 휴리스틱이 환경마다 다르게 실패할 수 있습니다.

기존 검증 범위에 미치는 영향을 줄이는 방법

생산 시스템에서는 어떤 방식이 더 멋진가보다 **어떤 변경이 기존 검증·승인 범위에 미치는 영향을 최소화하는가**가 중요합니다. 작은 어댑터, 별도 메모리, 검증 규칙은 전체 모델을 다시 학습하는 것보다 영향 범위를 설명하고 되돌리기 쉽습니다. 다만 작은 모듈도 안전하지 않은 출력을 증폭할 수 있으므로 독립 검증이 필요합니다.

2.5 실전 정책의 기본 조건: 폐루프 평가

행동을 한 번 생성하고 끝까지 재생하는 개루프 (open-loop) 방식은 실행 중 발생하는 변화에 즉시 대응하기 어렵습니다. 실제 환경에서는 사람이 끼어들고, 물체가 미끄러지고, 네트워크 지연이 바뀝니다. 정책이 자신의 행동 결과를 다시 관측하고, 예상과 다르면 수정해야 합니다.

폐루프는 특정 알고리즘의 이름이 아니라 시스템 구성 원리이자 평가 조건입니다. 화면의 정답 행동과 비슷한지를 재는 오프라인 지표만으로는 부족합니다. 행동이 다음 입력을 어떻게 바꾸는지까지 포함한 시뮬레이터 또는 실제 하드웨어에서 봐야 합니다.

속도만으로 안전을 판단할 수 없다

큰 모델이 느리다는 사실만으로 작은 모델이 항상 안전한 것은 아닙니다. 빠른 오답은 더 빠르게 사고를 만들 수 있습니다. 반대로 큰 모델의 깊은 추론도 제어 주기를 놓치면 가치가 없습니다. 속도와 지능을 같은 축에 놓기보다, 위험도에 따라 계산량을 배분하고 마지막 행동 권한을 별도 계층이 관리하는 것이 핵심입니다.

이 장에서 볼 숫자

제어 주기 준수율	정해진 시간 안에 행동 명령이 나온 비율과 마감 초과 분포
행동 경계 불연속	행동 묶음이 바뀔 때 속도·가속도·힘이 튀는 정도
중단 후 재개 시간	새 관측으로 계획을 수정하고 안정적인 행동으로 돌아가는 시간
기체별 적응 비용	새 로봇에 필요한 시연 수, 튜닝 시간, 안전 시험 범위

3

로봇은 무엇을 보고 있다고 믿는가

이 장의 한 문장

Physical AI 의 인지는 물체 이름을 맞히는 일이 아니라, 다음 행동이 사용할 수 있는 세계 상태를 만드는 일이다.

3.1 픽셀에서 행동 가능한 공간으로

"컵이 왼쪽에 있다" 는 문장은 사람에게 충분할지 몰라도 로봇에게는 부족합니다. 어느 좌표계의 왼쪽인지, 거리가 얼마인지, 손잡이가 어느 방향인지, 팔이 닿는지, 접근 경로가 비어 있는지 알아야 행동할 수 있습니다. **공간 접지 (grounding)**는 언어와 픽셀의 의미를 좌표, 방향, 도달 가능성, 충돌 여유로 연결하는 일입니다.

디지털 모델의 작은 환각은 틀린 설명으로 끝날 수 있습니다. 로봇에서는 즉시 비용이 됩니다. 물체의 종류는 맞혔지만 3cm 뒤를 잡으면 실패합니다. "테이블 위의 빈 공간" 을 말로는 찾았지만 팔의 부피와 손목 회전을 고려하지 않으면 충돌합니다. 따라서 Physical AI 의 인식은 분류 정확도만으로 평가할 수 없으며, 실제 **행동 가능성**까지 함께 확인해야 합니다.

의미 인식과 행동 가능성의 차이

먼저 이것부터 구분해봅시다. **무엇인가**와 **무엇을 할 수 있는가**는 다른 질문입니다. 전자는 의미 인식이고, 후자는 행동 가능성 (affordance) 입니다. 컵이라는 사실을 아는 것만으로는 부족합니다. 지금의 자세와 내용물, 온도, 주변 장애물까지 고려해 어디를 어떻게 잡을 수 있는지가 정책에 필요합니다.

3.2 왜 3D·BEV·LiDAR 가 다시 중요한가

카메라 영상은 풍부하고 값이 싸지만, 깊이와 가림에 구조적인 모호성이 있습니다. 주행과 이동 로봇에서는 자유 공간, 상대 속도, 시야 밖에서 나타날 수 있는 물체까지 다뤄야 합니다. 3 차원 점군, 조감도 표현 (BEV), 라이다, 깊이 정보는 이 모호성을 줄이는 도구입니다.

여기서 중요한 변화는 3 차원 인지가 독립적인 검출 단계로 끝나지 않고, 계획기와 월드모델이 공유하는 상태로 들어간다는 점입니다. 계획기는 "차가 있다" 보다 "어느 공간이 비었고, 어느 공간이 불확실하며, 2 초 뒤 점유될 가능성이 있는가" 를 알고 싶어 합니다.

3.2.1 Occupancy: 물체 목록보다 자유 공간

점유 표현은 공간을 비어 있음, 점유, 미관측으로 나눕니다. 형태가 정해지지 않은 장애물이나 처음 보는 물체도 "막혀 있다" 고 표현할 수 있어 충돌 회피와 경로 계획에 직접 쓰기 좋습니다. 여기에 의미와 시간축을 더하면 "보행자가 차지할 가능성이 큰 공간" 같은 위험 지도로 확장됩니다.

단점도 분명합니다. 조밀한 3D grid 는 메모리와 계산량이 큽니다. 먼 거리나 긴 미래일수록 불확실성이 급격히 증가합니다. 점유 상태를 잘 예측해도 다른 행위자의 의도까지 설명하지는 못합니다. 따라서 occupancy 는 모든 세계 표현을 대체하기보다, 기하와 위험 정보를 담는 공통 기반 표현에 가깝습니다.

세계 상태의 세 층

기하 층 위치, 깊이, 자유 공간, 충돌 여유, 속도

의미 층 객체, 관계, 역할, affordance, 작업 관련성

불확실성 층 보지 못한 영역, 센서 신뢰도, 미래 분포, 위험

좋은 계획기는 세 층을 함께 읽는다. 기하만 있으면 목적을 모르고, 의미만 있으면 물리에 약하며, 불확실성이 없으면 과신한다.

3.3 SLAM 의 지도는 공간 기억으로 확장된다

SLAM 은 로봇이 자신의 위치를 추정하면서 지도를 만드는 기술입니다. 전통적으로는 좌표와 기하의 일관성이 중심이었습니다. 장기 체화형 에이전트에서는 지도가 **지속적 공간 기억**으로 기능할 수 있습니다. 어디에 무엇이 있었는지, 무엇이 움직였는지, 어느 경로가 막혔는지, 마지막으로 확인한 시점이 언제인지가 계획에 필요합니다.

지도는 오래될수록 좋아지는 데이터베이스가 아닙니다. 동적 환경에서는 오래된 상태가 위험합니다. 의자를 어제 본 위치에 있다고 가정하면 충돌할 수 있습니다. 따라서 지도 수명주기, 갱신 주기, 불확실성, 재위치화 실패, 초기화 정책이 시스템 설계의 일부가 됩니다.

3.3.1 Gaussian splatting 의 위치

3D 가우시안 스플래팅은 장면을 명시적인 기본 요소 집합으로 표현해 실시간에 가깝게 렌더링합니다. 빠른 재현과 편집, 점진적 스트리밍이 강점이라 디지털 트윈, 센서 변환, 온라인 지도 표현에 활용하려는 움직임이 있습니다. 하지만 보기 좋

은 렌더링이 정확한 충돌 기하와 물리를 보장하지는 않습니다. 로봇용 지도가 되려면 의미 정보, 동적 갱신, 불확실성, 충돌 기하와 결합해야 합니다.

3DGS 의 현재 역할과 한계

3DGS 를 "새로운 지도" 라고 단정하면 너무 빠릅니다. 현재는 **렌더링과 상태 공유 비용을 낮추는 유망한 표현**으로 보는 편이 정확합니다. 장면을 잘 보여주는 능력과 로봇이 안전하게 부딪히지 않는 능력 사이에는 검증해야 할 거리가 남아 있습니다.

3.4 시각만으로는 접촉을 알 수 없다

물체가 미끄러지는 순간, 끼워 맞추기의 마지막 저항, 손가락에 걸리는 힘, 관절의 실제 위치는 카메라로 보이지 않거나 너무 늦게 보입니다. 그래서 시각만으로 관측하면 정교 조작은 본질적으로 부분관측 문제가 됩니다. 촉각, 힘·토크, 고유수용감각은 접촉 뒤의 상태를 알려줍니다.

최근에는 개별 센서와 작업마다 특징을 만들기보다, 대규모 촉각 데이터를 자기지도 학습해 여러 센서와 작업에 재사용하려는 흐름이 나타났습니다. 이것은 촉각을 보조 신호에서 여러 센서와 작업에 재사용되는 핵심 입력으로 끌어올릴 가능성을 보여줍니다. 다만 센서 표면, 해상도, 설치 위치가 다르면 분포가 크게 바뀌고, 카메라와의 시간 정렬도 어렵습니다.

3.5 센서를 더 달면 정말 더 똑똑해지는가

멀티모달 시스템은 RGB 영상, 깊이, 라이다, 촉각, 음향, 고유수용감각, 행동 이력을 함께 씁니다. 정보가 많아지는 것은 분명하지만 고장 방식도 늘어납니다. 한 센서가 늦거나 잘못 보정되면 서로 모순되는 상태가 생깁니다. 모든 감각 정보를 항상 같은 비중으로 결합하는 것은 좋은 설계가 아닙니다.

앞으로 중요한 것은 **신뢰도 기반 정보 선택**입니다. 접촉 전에는 시각을, 접촉 중에는 촉각과 힘을, 어두운 환경에서는 라이다를 더 신뢰하는 식으로 상황에 따라

센서별 신뢰도와 가중치를 조정해야 합니다. 센서가 빠졌을 때도 최소 기능을 유지하는 결측 센서 강건성이 필요합니다.

현장에서는

센서 하나의 성능보다 다음을 묻는 것이 좋습니다.

- 센서 시간이 50ms 어긋나면 정책 성능이 얼마나 떨어지는가?
- 보정값이 천천히 변할 때 분포 변화를 감지하는가?
- 센서 하나가 끊기면 즉시 정지하는가, 안전한 축소 모드로 가는가?
- 상태 추정에 사용한 근거와 불확실성을 로그로 남기는가?

이 장에서 볼 숫자

행동 기준 기하 오차	검출 오차가 아니라 집기·배치·여유 거리에서의 위치·각도 오차
미관측 공간의 불확실성 보정	미관측 영역을 빈 공간으로 오판하지 않는 정도와 불확실성 보정 성능
센서 결측 성능	카메라·깊이·촉각 일부가 없을 때 유지되는 성공률
접촉 감지 지연	미끄러짐·끼임·과도한 힘을 감지하고 반응하기까지의 시간

4

기억하고 상상하고 계획하는 로봇

이 장의 한 문장

장기 작업의 핵심은 긴 행동을 한 번에 만드는 것이 아니라, 상태를 보존하고 미래를 시험하며 실패한 부분만 되돌리는 것이다.

4.1 긴 입력창과 작업 기억은 다르다

컨텍스트 창을 늘리면 과거 영상을 더 많이 넣을 수 있습니다. 그러나 원시 이력을 보존하는 것과 정책에 필요한 상태를 유지하는 것은 다릅니다. 로봇은 컵을 어느 선반에서 꺼냈는지, 서랍을 이미 닫았는지, 사용자가 중간에 목표를 바꾸었는지, 같은 접근이 왜 실패했는지를 선택적으로 기억해야 합니다.

작업 기억에는 최소 네 종류가 있습니다.

- **감각 기억**: 최근 몇 초의 영상과 접촉 변화
- **에피소드 기억**: 어떤 순서로 무엇을 시도했고 결과가 어땠는지
- **의미 기억**: 물체, 장소, 관계, 규칙에 관한 압축된 지식
- **기술 기억**: 특정 조건에서 성공한 제어·복구 절차

저장보다 더 어려운 것은 갱신과 망각입니다. 오래된 위치를 유지하면 낡은 상

태 정보가 되고, 잘못된 실패 경험을 재사용하면 오류가 반복적이고 체계적으로 퍼질 수 있습니다. 메모리에는 출처, 시간, 기체, 센서 상태, 검증 여부가 따라다녀야 합니다.

기억이 유지해야 할 작업 상태

장기 작업의 기억은 과거 기록 전체가 아니라 현재 실행에 필요한 상태를 정확히 유지해야 합니다. 지금 하는 일에 필요한 정보가 선명하고, 틀린 내용은 수정되며, 누가 언제 갱신했는지 추적할 수 있어야 합니다.

4.2 월드모델은 행동 선택을 위한 예측 도구다

월드모델이라는 말은 너무 넓게 쓰입니다. 장면을 사실적으로 렌더링하는 모델, 행동에 따른 센서 변화를 예측하는 시뮬레이터, 목표에 맞는 행동을 고르는 계획기를 구분해야 합니다. Physical AI 의 계획·제어 관점에서 중요한 질문은 "영상이 얼마나 멋진가" 가 아니라 "이 예측이 더 나은 행동을 고르게 했는가" 입니다.

행동 후보 a 가 주어졌을 때 미래 상태 $\hat{s}_{t+1}$ 를 예측하고, 위험과 목표 달성도를 비교한다고 생각해봅시다.

월드모델을 계획에 쓰는 최소 형태

$$\hat{s}_{t+1} = f_\theta(s_t, a_t), \qquad a_t^\star = \arg\min_{a_t} \left[C_{\text{task}}(\hat{s}_{t+1}) + \lambda C_{\text{risk}}(\hat{s}_{t+1}) \right]$$

여기서 중요한 것은 f_θ 의 영상 품질이 아니라, 선택된 $a_t^\star$ 가 실제 폐루프에서 더 안전하고 더 높은 성공률을 보이는가 하는 점이다. λ 는 상황에 따라 위험 비용을 얼마나 크게 볼지 나타낸다.

장기 가상 실행은 작은 모델 오류를 누적합니다. 마찰을 조금 잘못 예측하면 몇 단계 뒤 물체 위치가 크게 틀어질 수 있습니다. 따라서 멀리 한 번에 예측하기보다 짧게 예측하고 실제로 관측하며 다시 계획하는 이동 지평 (receding-horizon) 구조가 현실적입니다.

4.3 추론의 문장과 행동은 일치하는가

로봇이 "먼저 장애물을 피하고 손잡이를 잡겠다" 고 올바르게 설명해도 실제 모터 명령은 장애물 쪽으로 향할 수 있습니다. 언어 추론의 품질과 행동의 일치는 별도 문제입니다. 실행 가능한 추론은 자연어 문장만이 아니라 좌표, 제약, 도달 가능 상태, 예상 결과, 검증 기록으로 내려와야 합니다.

여기서 런타임 검증기가 등장합니다. 정책이 만든 여러 행동 후보를 실행하기 전에 시뮬레이션하거나, 별도 모델과 규칙으로 결과를 검사하고, 위험한 후보를 차단합니다. 검증기도 틀릴 수 있으므로 그 판단을 절대적으로 신뢰해서는 안 됩니다. 정책과 다른 실패 모드를 가지는지, 거짓 양성과 거짓 음성을 어떻게 다루는지 봐야 합니다.

4.4 과업 계획과 동작 계획의 재결합

과업 계획은 "컵을 찾고, 잡고, 옮기고, 놓는다" 와 같은 단계 순서를 다룹니다. 동작 계획은 실제 관절과 경로가 충돌 없이 가능한지 계산합니다. 언어 모델은 고수준 계획 후보를 만드는 데 유용하지만, 동작 계획의 물리 제약을 자동으로 보장하지는 않습니다. 반대로 전통적 동작 계획기는 기하 제약을 정밀하게 다루지만 열린 환경의 의미와 모호한 목표를 처리하기 어렵습니다.

현실적인 구조는 고수준의 유연한 계획이 후보를 만들고, 기하·동역학·안전 제약이 실행 가능성을 좁히며, 결과를 재관측해 다음 하위 목표를 바꾸는 형태입니다. 이것이 계층 구조가 다시 중요해지는 이유입니다. 계층은 계산을 줄이는 장치일 뿐 아니라 **실패의 범위와 책임을 나누는 장치**입니다.

4.5 장기 작업은 신뢰성의 곱셈이다

교육용으로 단순한 계산을 해봅시다. 각 단계가 독립적으로 95% 성공하고 스무 단계가 모두 성공해야 한다면 전체 성공 확률은

$$0.95^{20} \approx 0.358$$

입니다. 약 35.8% 입니다. 실제 실패는 독립적이지 않으므로 이 숫자를 실험 결과로 읽으면 안 됩니다. 하지만 작은 단계 오류가 긴 작업에서 얼마나 빠르게 누적되는지 보여주는 좋은 직관입니다.

장기 작업 성공을 높이는 복구 구조

장기 작업의 해법은 단계 성공률을 100% 에 가깝게 만드는 것만이 아닙니다. 어디까지 했는지 checkpoint 를 남기고, 실패한 단계만 다시 시도하며, 잘못된 상태를 진단하고, 필요하면 사람에게 넘기는 구조가 전체 성공률을 더 크게 바꿀 수 있습니다.

4.6 복구 가능한 계획

좋은 장기 정책은 "실패하지 않는 계획" 보다 "실패해도 이어갈 수 있는 계획" 을 만듭니다. 각 하위 목표는 완료 조건, 예상 관측, 되돌릴 수 있는 범위, 상위 판단 이관 조건을 가져야 합니다. 복구도 다음과 같이 분리해서 볼 수 있습니다.

1. **탐지**: 예상과 실제 상태가 다르다는 사실을 빨리 알아챈다.
2. **진단**: 지각, 계획, 제어, 환경 변화 중 원인을 좁힌다.
3. **국소 수리**: 전체 초기화 없이 해당 단계만 다시 수행한다.
4. **안전한 중단**: 사전에 정한 자동 복구 범위를 벗어나면 멈추고 사람에게 넘긴다.
5. **학습**: 검증된 수정만 기술 기억과 데이터 파이프라인에 넣는다.

이 장에서 볼 숫자

상태 기억 정확도	오래된 상태와 현재 상태를 구분하고 진행 상황을 올바르게 복원하는 비율
계획 기여도	월드모델이나 검증기를 추가했을 때 실제 페루프 성공과 위험이 얼마나 바뀌는가
부분 완료율	전체 실패 안에서도 완료된 하위 목표와 보존된 작업의 비율
평균 복구 시간	오류 탐지부터 정상 실행 재개까지 걸린 시간
잘못된 기억 재사용	오염되거나 오래된 경험이 후속 작업에 전파된 비율

5

몸이 달라지면 지능도 달라진다

이 장의 한 문장

범용성은 모든 몸을 똑같이 다루는 능력이 아니라, 공통 지식과 몸별 제약을 올바르게 분리하는 능력이다.

5.1 조작은 종합시험이다

로봇 조작은 VLA, 3 차원 공간 접지, 촉각, 계획, 복구를 한 자리에서 시험합니다. 데이터 수집과 반복 실험이 상대적으로 가능하고 산업적 가치도 분명해, 범용 정책의 대표 무대가 되었습니다. 그러나 단순 집기·배치가 잘된다는 사실이 곧 실용적 조작을 뜻하지는 않습니다.

실험실 데모와 실제 생산·일상 작업을 가르는 요소는 변형 물체, 도구 사용, 조립, 가림, 작은 공차, 미끄러짐, 사람과의 협업입니다. 특히 접촉의 마지막 수 mm 에서 시각 기반의 대략적인 정책과 고주파 제어 사이의 간극이 드러납니다.

5.1.1 양손과 정교 조작

양손은 단순히 팔 하나를 더하는 문제가 아닙니다. 한 손이 만든 힘과 가림이 다른 손의 관측과 행동을 바꿉니다. 자유도가 늘수록 가능한 자세와 실패 경로가 폭발합니다. 고수준 정책이 역할과 순서를 정하고, 손 수준의 빠른 제어기와 촉각 피드

백이 접촉을 안정화하는 분업이 필요합니다.

정교 조작의 생산성 지표

정교 조작을 평가할 때 성공 여부만 보면 중요한 차이가 사라집니다. 접근 시간, 마지막 정렬 시간, 최대 힘, 미끄러짐 횟수, 대상 손상, 재시도 횟수, 작업 주기를 함께 봐야 생산성을 판단할 수 있습니다.

5.2 휴머노이드와 다족 보행

휴머노이드는 인간 환경의 도구와 통로를 그대로 쓸 수 있다는 기대를 받습니다. 동시에 이동, 균형, 조작을 분리하기 어렵습니다. 물건을 들면 질량 중심이 바뀌고, 문을 밀면 반력이 전신에 전달됩니다. **이동·조작 통합 (loco-manipulation)**은 이동과 조작을 하나의 전신 문제로 다룹니다.

시뮬레이션, 인간 영상, 대규모 동작 데이터가 좋아지며 전신 정책의 가능성이 넓어졌지만, 화려한 동작과 지속 가능한 제품은 구분해야 합니다. 에너지, 낙상, 관절 열, 유지보수, 사람 근접 안전, 바닥 조건 변화가 현장 병목입니다.

5.3 항법은 이동이 아니라 임무 수행이다

점 A 에서 B 로 가는 지점 간 항법은 오랫동안 연구되어 왔습니다. 서비스 로봇의 실제 항법은 목표를 찾고, 문과 엘리베이터를 이해하고, 사람의 흐름을 존중하며, 이동 뒤 조작을 이어가는 문제입니다. 언어, 의미 지도, 기억, 복구가 항법에 들어오는 이유입니다.

기체가 바뀌면 이동 능력도 달라집니다. 바퀴형, 다족, 휴머노이드, UAV 가 같은 목표 의미를 공유할 수는 있지만 가능한 경로와 위험은 다릅니다. 공통 임무 표현과 기체별 실행 가능성 판정 계층을 분리해야 합니다.

5.4 자율주행이 먼저 보여준 것

자율주행은 방대한 센서 로그, 페루프 시뮬레이션, 희귀 사건, 안전성 논증, 차량군 업데이트를 먼저 경험한 분야입니다. 최근의 종단간 모델과 월드모델은 인지–예측–계획의 경계를 다시 묻고 있습니다. 하지만 하나의 모델이 모든 기능을 맡는 구조보다 학습된 핵심 모델과 명시적 안전 범위가 결합된 형태가 현실적일 가능성이 큽니다.

주행에서 중요한 미래는 다른 행위자의 행동에 따라 달라집니다. 내가 차선을 바꾸면 뒤 차량의 속도가 달라질 수 있습니다. 따라서 각 행위자에게 하나의 최적 경로를 따로 부여하는 방식에서 벗어나, 자차의 행동에 따라 여러 행위자의 미래가 함께 어떻게 달라지는지를 조건부 분포로 예측해야 합니다.

자율주행에서 가져올 운영 구조

자율주행 사례를 다른 로봇에 그대로 옮기면 안 됩니다. 도로에는 비교적 명확한 규칙과 지도, 센서 배치가 있지만 가정과 공장의 접촉 작업은 상태와 목표가 더 다양합니다. 다만 **시뮬레이션–로그–안전 검증–로봇군 배포**를 잇는 운영 구조는 중요한 선행 경험을 제공합니다.

5.5 UAV 에 한꺼번에 드러나는 제약

UAV 는 빠른 시점 변화, 제한된 전력과 연산량, 통신 단절, 추락 위험을 동시에 안고 있습니다. 언어 기반 임무 계획기가 유용하더라도 최종 비행 안정성은 검증된 자동비행 제어기가 맡아야 합니다. 미래 장면을 예측하는 월드모델 기반 정책과 다기체 항법 정책은 흥미롭지만, 실환경의 바람과 GPS 음영, 인증 요건을 만족하는 지연 특성까지 검증해야 합니다.

5.6 기체 간 전이: 무엇을 옮길 것인가

로봇별로 고립된 데이터는 대규모 기반 정책 학습의 큰 장애물입니다. 여러 기체의 경험을 섞으면 공통 과업 의미와 시각적 동역학을 배울 수 있지만, 행동 공간·관절 구조·센서 배치가 다르면 오히려 성능이 나빠질 수 있습니다.

같은 악보도 피아노와 바이올린에서 연주법이 다릅니다. 곡의 구조는 공유할 수 있지만 손가락 동작과 실수의 위험까지 그대로 복사할 수는 없습니다. Physical AI 에서도 목표, 물체 관계, 시각적 중간 목표는 공유하되 운동학 어댑터와 기체별 제어기가 실행을 책임지는 구조가 유망합니다.

공통 지식과 몸별 지식

구분	공유하기 좋은 것	기체별로 남겨야 할 것
의미	목표, 객체 관계, 도구 역할	기체 능력과 금지 조건
공간	중간 목표, 상대 위치, 장면 구조	관절 한계, 도달 가능 범위, 점유 면적
행동	기술 이름, 성공 조건	모터 명령, 제어 이득, 접촉 전략
안전	위험 개념, 상위 판단 이관 규칙	속도·힘 한계, 정지 거리, 하드웨어 연동 차단 장치

이 장에서 볼 숫자

전체 주기 시간	인식부터 완료까지의 시간과 재시도 포함 처리량
기체 간 전이 손실	새 몸에서 추가 데이터 없이 유지되는 성능과 재학습 비용
접촉·낙상 비용	손상, 아차 사고, 최대 힘, 넘어짐, 안전 정지
상호작용 예측의 의사결정 손실	예측 오차가 최종 계획 결정에 끼친 비용

6

데이터는 쌓는 것이 아니라 운영하는 것이다

이 장의 한 문장

좋은 Physical AI 데이터의 기준은 양이 아니라 행동 정렬, 실패 범위, 출처, 그리고 안전한 수정 가능성이다.

6.1 실세계 데이터가 비싼 이유

웹의 이미지와 문장은 복사할 수 있지만 로봇 행동 데이터는 몸과 시간이 필요합니다. 사람이 시연하거나 로봇이 실제로 움직여야 하고, 충돌과 마모를 관리해야 하며, sensor 와 action 을 정확히 동기화해야 합니다. 성공 데이터는 비교적 모으기 쉽지만, 희귀하고 위험한 실패는 일부러 재현하기 어렵습니다.

그래서 Physical AI 의 데이터 문제는 단순히 규모를 키우는 일이 아닙니다. 다음 네 질문이 더 중요합니다.

1. 이 데이터의 행동은 실제로 어떤 목표와 조건에서 성공했는가?
2. 어떤 실패와 위험 구간이 빠져 있는가?
3. 어느 기체·센서·소프트웨어 버전에서 수집됐는가?

4. 수정된 정책이 실세계에서 다시 검증됐는가?

6.2 인간 영상, 시연, 선호는 서로 다르다

사람의 1 인칭 영상은 로봇 데이터보다 훨씬 큰 규모로 얻을 수 있고, 물체 사용과 장기 작업의 구조를 보여줍니다. 그러나 사람의 손과 로봇 그리퍼의 동역학은 다르며, 영상은 무엇을 했는지는 보여줘도 모터 명령과 힘 정보는 직접 제공하지 않습니다. 인간 영상은 의미와 시각적 중간 목표의 사전학습에 유용하고, 로봇 데이터는 실제 행동 정렬에 필요합니다.

시연은 정답 행동에 가까운 정보를 줍니다. 언어 교정은 "더 천천히", "손잡이를 먼저" 같은 기준을 전달합니다. 두 결과를 나란히 놓고 더 나은 쪽을 고르는 쌍대 선호 비교는 결과의 상대적 가치를 알려줍니다. 세 신호는 비용과 정보량이 다르며, 한 종류가 나머지를 완전히 대체하지 않습니다.

인간 피드백의 유형과 비용

사람의 피드백을 사용한 방법이 모두 선호 학습인 것은 아닙니다. 인간 영상, 자연어 교정, 현장 개입, 결과 선호는 서로 다른 감독 신호입니다. 책이나 제품 설명에서 이들을 구분해야 실제 데이터 비용과 편향을 이해할 수 있습니다.

6.3 생성·시뮬레이션은 통제된 실험 장치다

시뮬레이션과 생성 모델은 희귀 위험을 반복 재현하고 센서 구성을 바꾸며 서로 다른 조건의 결과를 시험할 수 있습니다. 실제 사고를 수천 번 재현할 수 없으므로 매우 중요합니다. 인터넷 영상에서 다중 시점 카메라와 라이다 형식의 로그를 합성하거나, 의미 점유 지도를 중심으로 영상과 포인트클라우드를 함께 생성하는 시도는 데이터 공급원의 경계를 넓힙니다.

그러나 합성 데이터는 실세계를 대체하지 않습니다. 시각적으로 사실적이면서 물리적으로 틀릴 수 있고, 시뮬레이터가 모르는 실패는 생성하지 못합니다. 따라

서 생성 데이터의 유용성은 이미지 품질보다 후속 정책의 성능과 실제 실행 위험을 기준으로 평가해야 합니다.

세 데이터원의 역할

데이터원	강점	약점	가장 좋은 용도
실로봇 로그	실제 물리·지연	비싸고 위험, 성공 편향	최종 검증과 현장 오차
인간 영상·교정	규모와 의미 구조	행동·힘 정보의 정렬 부족	사전학습, 중간 목표, 선호
시뮬레이션·생성	통제, 희귀 상황, 반복	현실 간극, 누락된 실패 유형	강건성 시험, 조건별 결과 비교

6.4 무학습 일반화라는 말을 분해해서 보자

"보지 못한 것에 일반화했다" 는 말은 무엇이 바뀌었는지에 따라 의미가 다릅니다. 새 물체, 새 장면, 새 과업 조합, 새 사용자, 새 기체는 난도가 다릅니다. 하나의 조건에서 추가 학습 없이 성공했다고 모든 변화에 강하다고 말할 수 없습니다.

앞으로는 일반화를 다음 축으로 분리해 보고해야 합니다.

- 객체와 외형
- 배경과 조명
- 과업의 새로운 조합
- 동역학과 접촉 조건
- 센서 구성
- 기체 형태와 구동 구조
- 장기 목표와 사람의 개입

일반화보다 더 중요한 질문은 실패할 때 무엇을 하는가입니다. 불확실성을 알고 거절하는지, 안전한 기본 동작으로 가는지, 사람에게 정확한 정보를 제공하는지가 제품의 가치입니다.

6.5 현장 적응은 작고 되돌릴 수 있어야 한다

마찰, 도구, 센서, 사용자 환경은 배포 후 바뀝니다. 고정 정책은 시간이 지나며 노후화됩니다. 온라인 적응은 매력적이지만 기존 능력을 잊게 하거나 승인 당시의 검증 범위를 벗어나게 할 수 있습니다. 전체 모델을 계속 바꾸기보다 제한된 정책 모듈과 잔차 보정기, 어댑터, 버전 관리 메모리, 검증된 기술 라이브러리만 갱신하는 방식이 현실적인 후보로 등장합니다.

검증 가능한 데이터 개선 순환

1. 배포 로그에서 실패와 아차 사고를 탐지한다.
2. 원인과 상태를 재현 가능한 기록으로 압축한다.
3. 시뮬레이션과 사람 검토로 수정 후보를 만든다.
4. 기존 작업 전체에 대해 회귀 시험을 한다.
5. 그림자 평가를 거쳐 일부 기체에 제한 배포한다.
6. 지표가 악화되면 자동으로 이전 버전으로 되돌린다.
7. 검증된 경험만 출처와 함께 재사용한다.

이 순환이 강해지면 경쟁력은 단일 모델 파일보다 데이터 운영 체계에서 나옵니다. 그러나 이것은 이미 증명된 산업 법칙이 아니라, 현재의 공개 사례가 이어질 때 예상되는 방향입니다. 데이터 축적이 진입 장벽이 되려면 실패를 빠르게 고치고 다른 현장에 안전하게 옮길 수 있어야 합니다.

이 장에서 볼 숫자

실패 데이터 비중	성공 시연뿐 아니라 복구·위험·극단 사례가 데이터에 포함된 정도
합성-실세계 간극	합성 데이터에서 좋아진 정책이 실제 페루프에서도 유지하는 개선량
업데이트 출처	어떤 데이터·기체·검증이 어느 버전에 영향을 주었는지 추적 가능성
회귀와 롤백 시간	새 학습이 기존 기능을 망가뜨린 정도와 이전 버전 복구 시간

7

한 대의 로봇에서 하나의 조직으로

이 장의 한 문장

여러 로봇의 지능은 에이전트 수가 아니라 역할, 공유 상태, 통신 장애, 버전 관리, 책임 경계에서 나온다.

7.1 협력은 통신보다 역할 설계다

여러 로봇을 연결하면 시야와 작업 능력을 확장할 수 있습니다. 창고, 교통, 재난 대응에서는 한 에이전트가 전체 환경을 볼 수 없습니다. 하지만 상태를 모두 공유한다고 협력이 생기지는 않습니다. 누가 어떤 목표를 맡고, 누가 충돌을 조정하며, 정보가 오래됐을 때 누구의 판단을 우선하는지 정해야 합니다.

다중 에이전트 연구는 흥미롭지만, 현재의 공개 근거를 넘어 "언어 기반 로봇 협력이 보편화됐다" 고 말하기는 이릅니다. 2026 년 하반기에는 로봇군 임무 조정, 공유 지도, 분산 안전, 통신량을 고려한 협력이 실제 운영 조건에서 얼마나 작동하는지를 보는 편이 타당합니다.

7.2 공유해야 할 것과 공유하지 말아야 할 것

모든 원시 센서 데이터를 클라우드에 올리면 대역폭과 개인정보 비용이 커집니다. 반대로 너무 압축하면 안전에 필요한 근거가 사라집니다. 공유 정보는 목적에 따라 나누는 것이 좋습니다.

공유 단위	예시	주의점
세계 상태	위치, 점유, 작업 상태, 위험 구역	기록 시각과 불확실성 표기가 필수
의도와 역할	다음 하위 목표, 우선순위, 예약 자원	계획 변경과 충돌 해결
기술과 수정	검증된 복구 절차, 어댑터, 규칙	기체 호환성과 되돌리기
사건 로그	아차 사고, 사람 개입, 실패 기록	개인정보와 책임 추적

7.3 중앙과 분산 사이

중앙 계획기는 전체 최적화를 하기 쉽지만 통신 지연과 단일 장애점이 생깁니다. 완전 분산은 강건하지만 역할 충돌과 전역 일관성을 관리하기 어렵습니다. 현실적인 시스템은 임무 배정과 로봇군 학습을 중앙에서 하되, 즉각적인 안전과 기본 임무는 각 기체가 독립적으로 유지하는 혼합형 구조가 됩니다.

로봇군에 필요한 인계 정보와 실패 절차

병원은 의사가 많아서 똑똑한 것이 아닙니다. 진료 기록, 역할, 인계, 응급 절차가 있기 때문에 조직적으로 움직입니다. 로봇군도 마찬가지입니다. 공유 메모리보다 더 중요한 것은 **인계 가능한 상태와 실패 절차**입니다.

7.4 좋은 업데이트도 대규모 실패가 될 수 있다

한 로봇에서 성공한 보정을 로봇군 전체에 배포하면 개선 속도가 빨라집니다. 동시에 잘못된 수정이 모든 기체로 퍼질 수 있습니다. 기체별 능력이 다르면 같은 기술도 위험합니다. 그래서 모델 등록부, 기체 호환성 검사, 제한 배포 집단, 단계적 확대, 긴급 되돌리기가 Physical AI 운영의 기본 인프라가 됩니다.

이 장에서 볼 숫자

통신 단절 성능	클라우드와 연결이 끊겼을 때 유지되는 안전과 핵심 기능
상태 신선도	공유 지도·과업 상태의 지연과 오래된 정보 사용률
조정 비용	협력으로 얻은 처리량 대비 통신·대기·충돌 해결 비용
오류 확산 반경	잘못된 업데이트가 영향을 준 기체 수와 차단 시간

8

데모를 제품으로 바꾸는 법

이 장의 한 문장

현장에서는 실패를 완전히 없애는 시스템보다, 실패의 범위를 알고 빨리 감지하며 안전하게 복구하는 시스템이 더 가치 있다.

8.1 평균 성공률이 숨기는 것

평균 성공률은 짧고 명확하지만 중요한 차이를 숨깁니다. 쉬운 과업이 많은지, 실패가 파손을 만드는지, 몇 번 재시도했는지, 사람이 얼마나 개입했는지, 작업 시간이 얼마나 걸렸는지 알 수 없습니다. 선별된 영상은 더 심합니다. 전체 시도 수와 초기화 비용이 보이지 않습니다.

Physical AI 의 평가는 과업 성공률을 버리는 것이 아니라 운영 지표로 확장하는 일입니다. 성공과 실패 여부뿐 아니라 진행률, 처리량, 에너지, 사람 개입, 복구, 아차 사고, 최악 구간의 지연을 함께 봐야 합니다.

성능을 운영가치로 번역하기

$$\text{운영가치} \approx \frac{\text{완료 작업} \times \text{작업 가치}}{\text{사람 개입} + \text{정지 시간} + \text{에너지} + \text{손상 위험} + \text{정비 비용}}$$

정확한 회계식이 아니라 판단 틀이다. 성공률이 같아도 개입과 복구 시간이 다르면 총소유비용은 크게 달라진다.

8.2 강건성과 일반화는 무너지는 조건으로 설명하라

모델 규모가 커지면 다양한 사전지식을 얻을 수 있지만, 학습 분포 밖 조건에서의 강건성이 자동으로 보장되지는 않습니다. 강건성은 "새 환경에서도 잘했다" 보다 어떤 변화에 얼마나 무너지는지로 기술해야 합니다. 조명, 물체, 배경, 카메라, 지연, 마찰, 사람의 행동을 따로 바꾸어 시험하고 그 조합도 확인해야 합니다.

또한 모델의 확신 정도가 실제 실패 가능성과 맞는지 확인해야 합니다. 자신이 없을 때 속도를 줄이거나 물러나고, 질문하거나 사람에게 넘기는 **행동 보류** 능력도 범용성의 일부입니다.

8.3 안전은 실행 보증 계층이다

안전은 충돌 방지 센서 하나로 끝나지 않습니다. "뜨거운 물체를 잡지 말라", "사람의 약을 다른 사람에게 주지 말라" 같은 의미 수준의 안전과 물리적 속도·힘 한계가 함께 있습니다. 내부 판단 근거를 들여다보기 어려운 기반 정책의 출력을 구동기에 그대로 연결하면 책임 경계가 흐려집니다.

실행 보증 구조는 다음 역할을 포함합니다.

- 능력의 경계와 금지 상태의 명시
- 실행 전 후보 검사와 속도·힘 제한
- 실행 중 위험 감시와 독립된 정지 경로
- 사람의 우선 개입과 상위 판단 이관
- 사건 로그와 재현 가능한 기록

- 변경 승인, 사후 모니터링, 이전 버전으로 되돌리기

안전 기준은 제품과 용도에 따라 달라진다

산업용 로봇 응용·셀을 다루는 ISO 10218-2:2025 는 중요한 안전 기준이지만, 서비스·의료·소비자·공중 로봇 전체에 그대로 적용되는 만능 규칙은 아닙니다. EU 의 AI 규정도 모든 로봇을 자동으로 같은 위험 등급으로 취급하지 않습니다. 제품의 용도, 배치 환경, 다른 제품 규정과의 결합을 별도로 검토해야 합니다.

8.4 효율은 안전과 경제성의 문제다

모델 압축과 기기 내 실행은 단지 비용 절감이 아닙니다. 네트워크가 끊겨도 동작하고, 예측 가능한 지연을 만들며, 개인정보를 기기 내부에 보관할 수 있습니다. 반면 엣지 기기의 발열·메모리·배터리 제약은 제어 주기와 센서 처리량을 제한합니다.

앞으로는 모델 단독 압축보다 센서–토큰–네트워크–하드웨어–스케줄러의 공동 설계가 중요해집니다. 위험이 낮은 이동 구간에서는 적은 계산을 쓰고, 접촉과 사람이 가까운 구간에서는 더 깊은 추론과 검증을 쓰는 적응형 계산이 현실적입니다.

8.5 실패를 다루는 네 단계

실패는 하나의 분류표로 끝나지 않습니다. 감지했지만 원인을 모를 수 있고, 원인은 알지만 복구할 권한이 없을 수 있습니다. 평가도 분리해야 합니다.

1. **탐지**: 실패 징후를 얼마나 빨리 알아차리는가
2. **진단**: 지각·계획·제어·환경 중 원인을 얼마나 정확히 찾는가
3. **복구**: 국소 행동으로 정상 상태에 얼마나 자주 돌아오는가
4. **상위 판단 이관**: 자동 권한 밖에서 안전하게 멈추고 사람에게 정보를 넘기는가

데모에서 제품으로 넘어갈 때의 지표

운전면허 시험에서 한 번 코스를 완주한 것과 택시 차량군을 운영하는 것은 다릅니다. 후자에는 차량 상태, 사고 기록, 운전자 개입, 정비 시간, 보험 비용이 들어갑니다. 로봇도 데모를 제품으로 바꾸는 순간 같은 종류의 질문을 받습니다.

8.6 평가자가 독립적이어야 하는 이유

모델을 만든 팀이 잘 아는 과업과 환경에서 평가하면 숨은 적응과 선택 편향이 생깁니다. 독립적인 분산 실로봇 평가, 이중맹검 비교, 학습과 조정에 쓰지 않은 환경, 장기 일상 과업은 범용성 주장을 더 엄격하고 의미 있게 만듭니다. 시뮬레이터가 접촉과 지연을 충분히 반영하는지는 실기체로 교차 확인해야 합니다.

제품 검토표

전체 과업 성공률	부분 동작이 아니라 초기 상태부터 종료 조건까지 완수
사람 개입률	작업당·시간당 사람 개입과 개입 이유
복구 성공률	초기화 없이 복구한 비율과 평균 복구 시간
꼬리 지연	최악 구간의 인지–행동 지연
안전 비용	충돌, 아차 사고, 최대 힘, 위험 행동 제안과 실제 실행
가동률	작업 가능 시간 대비 실제 가동 시간
변경 실패율	업데이트가 회귀·사고·되돌리기를 만든 비율
총비용	하드웨어, 데이터, 검토, 정비, 원격 개입을 포함한 현장 비용

9

2026 년 하반기에서 2030 년까지

이 장의 한 문장

모델 이름은 빠르게 바뀌지만 정책 코어, 세계 상태, 메모리, 기술 라이브러리, 제어기, 검증기, 운영 로그라는 역할은 남는다.

9.1 하반기: 통합을 증명하는 시간

2026 년 상반기까지 공개된 사례들은 범용 정책, 메모리, 월드모델, 실행 중 검증기, 현장 보정, 기체 간 전이가 연결될 수 있음을 보여줬습니다. 하반기의 핵심은 이 조합이 통제된 데모를 넘어 얼마나 오래, 여러 환경에서, 낮은 개입으로 작동하는지 확인하는 일입니다.

다음 세 가지 결과가 중요합니다. 첫째, 장기 과업에서 중간 상태 저장과 복구가 실제 전체 성공률을 높이는가. 둘째, 월드모델과 검증기가 영상 지표가 아니라 실제 실행 위험과 잘못된 계획 선택으로 생긴 손실을 줄이는가. 셋째, 기기 내 실행과 빠른 제어기가 지연을 낮추면서 범용 정책의 의미 판단을 보존하는가.

9.2 2027–2028: 모듈화와 검증

현재의 흐름이 이어진다면 범용 정책은 모든 모터를 직접 제어하기보다 여러 전문 모듈을 호출하는 정책 코어로 자리 잡을 가능성이 있습니다. 메모리, 세계 상태, 기술 라이브러리, 검증기, 하드웨어 제어기는 명확한 인터페이스를 갖고, 기체별 어댑터와 현장 보정 계층이 중요해질 것입니다.

이 시기에는 벤치마크와 안전성 논증도 더 구조화될 가능성이 큽니다. 하나의 평균 성공률보다 능력의 경계, 환경 변화 축, 사람 개입, 복구, 꼬리 지연, 업데이트 출처와 이력이 기본 보고 항목이 되는지를 지켜봐야 합니다.

9.3 2029–2030: 운영체제형 계층

장기적으로 Physical AI 는 단일 모델보다 운영체제와 비슷한 계층으로 정착할 수 있습니다. 다양한 기반 모델을 바꿔 끼우더라도 세계 상태, 기술 인터페이스, 실행 권한, 기록, 배포 통제는 남습니다. 현장별로 검증된 데이터와 복구 지식이 쌓이면, 모델 자체보다 안전한 개선 루프가 진입 장벽이 될 수 있습니다.

그러나 이것은 조건부 전망입니다. 단일 통합 모델이 지연, 장기 기억, 기체 전이, 안전 검증을 한꺼번에 해결하고 더 낮은 총비용을 보인다면 모듈화 전망은 약해질 수 있습니다. 반대로 전문 모듈이 너무 많아 구성 요소 사이의 오류와 통합 비용이 커진다면 범용 정책 코어의 직접 제어 범위가 다시 넓어질 수 있습니다.

앞으로 남을 가능성이 큰 일곱 인터페이스

1. **목표 인터페이스:** 사람이 원하는 목표와 금지 조건
2. **세계 상태 인터페이스:** 기하·의미·불확실성의 공통 상태
3. **메모리 인터페이스:** 저장·검색·갱신·망각·출처
4. **기술 인터페이스:** 기체별로 실행 가능한 행동과 성공 조건
5. **안전성 입증 인터페이스:** 권한, 검증기, 정지, 인간 개입

6. **학습 인터페이스**: 데이터와 업데이트의 승인 범위
7. **운영 인터페이스**: 배포, 관측, 제한 시험, 되돌리기, 감사

9.4 이 전망을 뒤집을 신호

좋은 전망은 반증 조건을 가집니다. 다음 신호가 나타나면 이 책의 중심 해석을 수정해야 합니다.

- 긴 작업에서 메모리와 계층 구조가 단순히 입력 맥락을 늘리는 방법보다 일관되게 낫지 않다.
- 월드모델의 품질 향상이 실제 계획과 위험 지표에 거의 기여하지 않는다.
- 실행 중 검증기가 지연과 잘못된 차단을 늘릴 뿐 전체 안전을 개선하지 않는다.
- 기체 간 전이 학습이 기체별 전문 정책보다 총데이터와 검증 비용을 줄이지 못한다.
- 현장 적응이 회귀와 인증 비용 때문에 대부분 금지되고, 사전 검증된 오프라인 업데이트만 남는다.
- 범용 정책보다 작고 고정된 과업별 시스템이 장기간 총소유비용에서 계속 우세하다.

모델이 바뀌어도 남는 인터페이스

2030 년의 모델 이름을 맞히려고 하지 마십시오. 대신 그때도 필요한 인터페이스를 보십시오. 목표는 어디서 들어오고, 세계 상태는 누가 만들며, 행동 권한은 누가 주고, 실패는 어디에 기록되고, 업데이트는 어떻게 되돌리는가. 이 질문들은 모델 이름이 바뀌어도 남습니다.

9.5 연구자와 조직을 위한 질문

9.5.1 연구자에게

새 모듈이 실제 페루프 성능을 얼마나 바꿨는가? 평균뿐 아니라 실패 분포와 극단 구간도 제시하는가? 시스템에서 어떤 역할을 바꾸었고 다른 구성 요소와의 접점은 무엇인가? 반증 가능한 조건을 제시하는가?

9.5.2 제품 책임자에게

데모 성공률이 아니라 하루의 처리량과 사람 개입은 얼마인가? 어떤 상태에서 자동 행동 권한을 회수하는가? 사고 trace 를 재현할 수 있는가? 새 버전의 회귀 시험과 rollback 은 몇 분 또는 몇 시간 안에 가능한가?

9.5.3 회사 운영자에게

로봇 가격보다 데이터 수집, 원격 개입, 검토, 현장 통합, 유지보수, 보험과 책임 비용이 더 클 수 있습니다. Physical AI 의 사업성은 한 대의 지능 점수가 아니라 로봇군 전체의 **총소유비용**으로 판단해야 합니다.

2026 년 하반기 관찰 대시보드

정책	새 과업 조합, 기체 전이, 행동 지연, 비동기 실행
세계 상태	3 차원·점유·촉각 정보가 계획에 기여하는 정도와 불확실성 보정
장기성	메모리 검색, 중간 상태 저장, 부분 완료, 복구
월드모델	조건별 결과를 비교하는 계획과 실제 페루프 위험 감소
데이터	인간·로봇·합성 데이터의 정렬과 재검증
신뢰성	사람 개입, 행동 보류, 아차 사고, 실행 중 검증
운영	엣지 실행, 가동률, 변경 실패, 제한 배포, 되돌리기, 현장 총비용

에필로그: 로봇에게 책임을 묻다

앞으로 로봇이 더 영리해질 것이라는 사실은 그리 놀랍지 않습니다. 시각 모델은 더 넓은 장면을 이해하고, 언어 모델은 더 복잡한 목표를 해석하며, 정책은 더 다양한 몸을 움직일 것입니다.

정말 중요한 변화는 따로 있습니다. 우리가 그 영리함을 어디까지 믿고, 어느 상태에서 속도를 낮추며, 어디에서 멈추게 하고, 실패한 뒤 무엇을 배우게 할 수 있는가입니다. 로봇이 기억한다면 잘못된 기억을 지울 수 있어야 하고, 미래를 상상한다면 그 상상이 실제 판단을 개선했는지 확인해야 하며, 계속 학습한다면 어제 승인한 시스템으로 되돌릴 수 있어야 합니다.

Physical AI 를 큰 모델 하나로 보면 매달 새로운 이름에 흔들립니다. 페루프로 보면 역할이 보입니다. 관측, 세계 상태, 기억, 계획, 정책, 제어, 검증, 복구, 운영. 이 역할들을 연결하고 경계를 설명할 수 있는 조직이 데모를 일로 바꿉니다.

> *Physical AI* 의 미래는 지능의 크기보다, 그 지능이 만든 결과를 다시 확인하고 실패를 복구하는 페루프의 완성도에 달려 있다.

다섯 변곡점의 심화 분석

다섯 변곡점: 왜 2026 년 중순인가

본문에서 우리는 Physical AI 를 관측, 세계 상태, 기억, 계획, 정책, 제어, 검증, 복구가 이어지는 폐루프로 읽었습니다. 이제 한 걸음 물러나 질문해봅시다. 왜 이 역할들이 2026 년 중순에 한꺼번에 중요해졌을까요?

2024–2025 년의 주요 관심이 "대형 VLA 하나로 여러 행동을 수행할 수 있는가"에 있었다면, 2026 년 중순의 질문은 전체 시스템으로 넓어졌습니다.

> 새로운 상황에 실제로 재사용할 수 있고, 장시간 실패를 관리하며, 객관적으로 평가되고, 안전성을 입증할 수 있는 전체 로봇 시스템을 어떻게 만들 것인가?

다섯 변곡점은 서로 독립된 유행이 아닙니다. 정책의 적용 범위가 넓어지면서 계획·기억·검증·평가·책임이 함께 하나의 시스템 과제로 떠올랐습니다.

01 범용 정책이 "새 조합"을 다루기 시작

새 물체를 알아보는 일반화에서, 배운 기술을 처음 보는 순서로 묶고 다른 로봇의 몸에서도 재사용하는 일반화로 질문이 커졌습니다.

02 월드모델이 실행 구조에 들어오기 시작

미래 영상을 보기 좋게 생성하는 단계를 넘어, 행동 후보를 미리 시험하고 정책 학습과 평가에 연결하려는 흐름이 강해졌습니다.

03 메모리·계층·검증기가 독립된 역할로 분리

긴 입력창 하나보다 작업 상태, 하위 작업, 빠른 제어기, 실행 승인, 복구를 분리한 구조가 장기 작업의 현실적인 후보로 등장했습니다.

04 실로봇 평가가 데모와의 간극을 드러냄

선별된 성공 영상과 평균 성공률만으로는 범용성을 판단하기 어렵습니다. 분산·장기·안전 평가가 실패 분포와 복구 능력을 요구합니다.

05 표준과 규제가 안전성 입증을 설계 요구로 전환

안전하다는 주장보다 인간 감독, 기록, 강건성, 회귀 시험, 사후 모니터링을 연결한 증거 체계가 중요해졌습니다.

서로 연결된 다섯 변화

다섯 변화는 따로 움직인 유행이 아닙니다. 범용 정책의 적용 범위가 넓어지면서 장기 실행의 계획·기억·검증 문제가 함께 커졌고, 실제 성능 측정과 안전성 입증 요구도 뒤따랐습니다. 서로 다른 연구 흐름이 하나의 시스템 문제 안에서 연결되기 시작한 것입니다.

01. 일반화의 단위가 물체에서 과업과 몸으로 커졌다

예전의 일반화와 지금의 일반화

기존 로봇 연구에서 일반화는 주로 시각적 변화에 대한 강건성을 뜻했습니다. 학습 때 없던 색의 컵을 집거나, 조명과 배경이 달라져도 같은 동작을 수행하거나, 물체 위치가 조금 달라져도 성공하는 식입니다. 이것은 여전히 중요하지만, 물체를 알아보는 능력과 새로운 과업을 수행하는 능력은 다릅니다.

2026 년의 중요한 질문은 **조합적 일반화 (compositional generalization)**입니다. 이미 배운 기술을 한 번도 보지 못한 순서와 조건으로 조합할 수 있는지를 묻습니다.

과업 조합이 만드는 새로운 난도

로봇이 다음 다섯 기술을 각각 배웠다고 합시다.

1. 서랍 열기
2. 컵 집기
3. 물체 옮기기
4. 식기세척기 문 열기
5. 문 닫기

학습 중에는 이 기술들을 개별적으로만 봤습니다. 그런데 처음 보는 지시가 들어옵니다.

> "서랍에서 빨간 컵을 꺼내 식기세척기에 넣고 문을 닫아."

부품은 배웠지만 이 순서와 조합은 처음입니다. 로봇은 현재 상태를 읽고, 필요한 기술을 선택하고, 완료 조건을 확인하며, 중간 실패에서 복구해야 합니다. 이것이 물체 수준의 일반화보다 훨씬 큰 문제인 이유입니다.

몸이 달라지면 문제가 한 단계 더 커집니다. 단일 팔에서 양팔로, 고정형 팔에서 이동형 조작기로, 로봇 팔에서 휴머노이드로 옮기면 관절 수, 도달 영역, 센서 배치, 제어 주기, 안전 한계가 달라집니다. 공통 지식은 재사용하되 기체별 실행 가능성 판정과 제어기를 다시 연결해야 합니다.

CrossFormer는 여러 로봇 기체를 하나의 정책으로 다루는 방향을 보였고, LAP은 언어로 표현한 행동을 이용해 학습하지 않은 기체로 옮기는 문제를 다룬 사전공개 연구입니다. 후자는 최신 결과이므로 후속 검증이 필요하지만, 질문의 단위가 "새 물체" 에서 "새 몸" 으로 커지고 있음을 보여줍니다.

사전학습 정책의 가치는 적응 비용으로 측정된다

사전학습된 범용 정책의 가치를 한 번의 최고 성공률로만 보면 중요한 경제성이 빠집니다. 새 로봇과 새 작업에 옮길 때 필요한 전체 비용을 보아야 합니다.

배포 비용의 구성 요소

$$C_{\text{배포}} = C_{\text{데이터}} + C_{\text{적응}} + C_{\text{보정}} + C_{\text{안전 검증}} + C_{\text{평가}}.$$

좋은 사전학습 정책은 사전학습 성능만 높은 모델이 아니라, 새로운 현장에서 데이터·보정·안전 검증·평가 비용의 합을 낮추는 모델입니다.

그래서 앞으로는 단일 무학습 전이 수치보다 적응 곡선이 중요합니다. 1 회, 10 회, 50 회 시연에서 성능이 어떻게 변하는지, 새 기술을 배운 뒤 기존 기술을 잊지 않는지, 위험한 상황에서 스스로 거절하는지를 함께 봐야 합니다.

일반화의 단위가 커졌다

"새 물체도 집는다" 에서 "배운 기술을 새 순서로 조립하고, 다른 몸을 가진 로봇에서도 적은 비용으로 재사용한다" 로 일반화의 단위가 커졌습니다.

02. 월드모델은 미래 영상보다 행동의 결과를 예측한다

보기 좋은 미래와 쓸 수 있는 미래

초기의 비디오 월드모델은 현재 영상을 입력받아 다음 프레임을 그럴듯하게 만드는 데 초점을 두었습니다. 하지만 로봇은 여러 행동 가운데 하나를 골라야 합니다. 그래서 필요한 것은 현재 상태와 행동 후보를 조건으로 한 미래 예측입니다.

행동 조건부 가상 실행

$$\hat{s}_{t+1:t+H} = f_\theta(s_t, a_{t:t+H-1})$$

현재 상태 s_t 에서 행동 열 $a_{t:t+H-1}$ 을 실행했을 때, 앞으로 관측하거나 도달할 상태를 예측합니다.

월드모델을 이용한 행동 후보 비교

컵 주변에 장애물이 있다고 합시다. 정책이 세 후보를 만듭니다.

- **후보 A**: 정면에서 빠르게 잡는다.
- **후보 B**: 측면에서 천천히 접근한다.
- **후보 C**: 주변 장애물을 먼저 치운다.

월드모델 안에서 세 후보를 짧게 실행해보고 충돌, 컵의 전도, 목표 진전, 후속 행동 가능성을 비교합니다. 실제 로봇에는 가장 유리한 후보만 보냅니다. 이때 월드모델은 영상 생성기가 아니라 **행동 후보를 비교하는 가상 실행 환경**입니다.

정방향 동역학은 현재 상태와 행동으로 다음 상태를 예측하고, 역동역학은 목표 상태에 필요한 행동을 추정합니다. 센서 시뮬레이션은 RGB, 깊이, 점군, 촉각, 고유수용감각, 힘·토크처럼 로봇이 실제로 얻게 될 관측을 생성합니다. 이런 가상 실행 결과는 정책 학습과 평가에도 활용됩니다.

DINO-WM은 원시 픽셀 전체를 재구성하는 대신 사전학습된 시각 특징의 미래를 예측하고, 목표 특징에 도달하는 행동열을 최적화한 계획 사례입니다. WorldGym은 행동을 조건으로 미래 영상을 생성하는 모델에서 여러 정책을 가상 실행해 순위를 추정하는 문제를 다룹니다.

월드모델의 과신이 가장 위험하다

그럴듯한 영상과 물리적으로 올바른 미래는 다릅니다. 생성 장면에서는 손가락이 컵을 잡은 것처럼 보여도 실제로는 마찰이 부족하거나, 기하 구조가 서로 관통하거나, 힘이 지나치게 클 수 있습니다. 학습 분포 밖의 행동에서는 모델 오차가 긴 가상 실행을 따라 누적됩니다.

월드모델의 허점을 이용한 행동을 시험해야 한다

월드모델을 평가할 때 영상 유사도나 사람의 선호만으로는 부족합니다. 접촉 상태, 제약 위반, 목표 진전, 불확실성 보정, 잘못된 계획 선택으로 생긴 손실을 봐야 합니다. 특히 정책이 월드모델의 허점을 이용해 현실에서는 실패할 행동을 고르는지 시험해야 합니다.

하반기에 볼 숫자

계획 선택 손실	월드모델이 고른 행동과 실제 최선 행동의 비용 차이
예측 길이별 오차	예측 길이가 늘어날 때 상태·위험 오차가 누적되는 속도
분포 밖 불확실성 보정	학습 분포 밖 행동에서 불확실성이 실제 오류와 맞는 정도
정책 순위 일치도	가상 평가 순위와 실로봇 평가 순위의 일치

월드모델의 역할이 실행으로 확장됐다

월드모델은 “미래 영상을 그리는 모델” 에서 “행동을 미리 시험하고, 정책을 학습하며, 로봇을 평가하는 가상 실행 환경” 으로 이동하고 있습니다.

03. 긴 입력창보다 역할과 연결 규칙이 필요하다

커피 만들기에서 무엇을 기억해야 하는가

과거 영상을 길게 넣는다고 장기 작업이 자동으로 해결되지는 않습니다. 커피를 만드는 로봇이 기억해야 하는 것은 영상 전체가 아니라 구조화된 작업 상태입니다.

장기 작업에 필요한 상태 변수

- 컵을 꺼냈는가?
- 컵 안이 비어 있는가?
- 커피 캡슐을 넣었는가?
- 기계 전원을 켰는가?
- 물이 충분한가?
- 직전 행동은 성공했는가?
- 현재 어느 하위 작업을 수행 중인가?

긴 영상 이력을 모두 다시 읽게 하기보다, 이 상태를 갱신하고 출처와 변경 이력을 붙이는 편이 계획과 복구에 직접 유용합니다.

고수준 계획기와 모터 제어기의 시간 규모도 다릅니다. 계획기는 수 초 간격으로 목표를 분해해도 되지만, 접촉과 균형은 수 ms 단위로 반응해야 합니다. 검증기는 후보 행동이 현재 목표와 상태에 맞는지 확인하고, 복구 제어기는 실패 뒤 되돌리기, 재시도, 재계획을 담당합니다.

역할	시간·상태	책임
메모리·상태	사건·객체·과업 이력	지금까지 무엇이 일어났는지 유지
고수준 계획기	느린 하위 작업 주기	목표 분해와 다음 단계 선택
빠른 제어기	빠른 제어 주기	실제 모터 명령과 접촉 안정화
검증기	실행 전·중 검사	목표·실행 가능성·위험 승인
복구 제어기	실패 사건 기반	되돌리기, 재시도, 재계획, 사람 호출

검증기는 생성기와 다른 질문을 한다

정책은 가능성 높은 행동을 생성합니다. 검증기는 그 행동이 지금 실행 가능한지, 안전한지, 목표를 진전시키는지, 이전 실패를 반복하는지를 묻습니다.

생성과 검증의 분리

$$\text{생성기} \longrightarrow \{a_1, a_2, \ldots, a_K\} \longrightarrow \text{검증기} \longrightarrow a^\star$$

후보를 많이 만드는 능력과 올바른 후보를 승인하는 능력은 같지 않습니다.

HAVE는 행동 생성과 과거 이력을 이용한 검증을 분리해 이전 상호작용에 기반한 후보 선택을 다뤘습니다. HELM은 장기 과업의 메모리, 검증, 복구 격차를 분해한 사전공개 연구입니다. 최신 결과는 후속 검증이 필요하지만, 단순히 입력창을 늘리는 것과 역할을 분리하는 것의 차이를 명확하게 보여줍니다.

실행 승인: 구동기 앞의 마지막 관문

실행 전 안전 게이트의 확인 항목

정책이 "팔을 30cm 전진하고 그리퍼를 닫아라" 라는 명령을 만들었다고 합시다. 실행 직전의 승인 계층은 다음을 확인합니다.

- 사람과의 최소 거리를 위반하는가?
- 관절 한계와 속도·힘 한계를 넘는가?
- 충돌 가능성과 불확실성이 허용 범위 안인가?
- 현재 하위 작업과 일치하는가?
- 이전에 실패한 행동 패턴을 반복하는가?

통과하면 구동기로 보내고, 아니면 정지, 재계획, 사람 호출 중 하나를 선택합니다.

이는 고전적 모듈형 로봇공학으로 완전히 돌아간다는 뜻이 아닙니다. 각 역할은 신경망 모델로 구현되어 함께 학습될 수 있습니다. 중요한 것은 **역할·상태·권한·연결 규칙을 설명할 수 있다**는 점입니다.

역할과 실행 권한을 분리한다

"하나의 거대한 모델에 모든 기억과 판단과 제어를 맡기자" 에서 "기억하는 부품, 계획하는 부품, 빠르게 제어하는 부품, 검사하고 복구하는 부품의 책임을 나누자" 로 이동하고 있습니다.

04. 평균 성공률 하나로는 범용성을 평가할 수 없다

데모 영상이 말하지 않는 것

성공한 실행 사례 몇 개만 보면 로봇이 완성된 것처럼 보입니다. 그러나 총 시도 수, 실패 영상, 사람이 만든 초기 조건, 중간 모델 수정, 연속 작동 시간, 위험 행동은 보이지 않습니다. 열 번 중 한 번 성공한 장면만 고르면 영상은 완벽할 수 있습니다.

평균 성공률도 충분하지 않습니다. 같은 80% 가 전혀 다른 시스템을 가릴 수 있습니다.

평균 성공률이 숨기는 실패 분포

	정책 A	정책 B
분포	환경 전반에서 약 80%	쉬운 환경 100%, 특정 조건 0%
실패	경미한 실패, 국소 복구	물체 낙하, 사람 쪽 이동
개입	낮고 예측 가능	특정 조건에서 개입 급증
배포 해석	한계를 관리하기 쉬움	평균만 보면 위험이 가려짐

범용 정책을 평가하려면 환경·과업·기체별 성능 분포와 신뢰구간, 꼬리 실패율을 함께 봐야 합니다. 연속 수행에 따른 성능 저하, 교란 후 복구, 사람 개입, 안전 위반의 심각도와 평균 복구 시간도 필요합니다.

평가도 자동화되고 분산된다

AutoEval은 성공 판정과 장면 초기화를 자동화해 실제 로봇 정책을 반복 평가하는 구조를 제안했습니다. 해당 연구팀은 사람의 감독 시간을 크게 줄이고 장시간 평가할 수 있다고 보고했습니다. RoboArena는 여러 기관에서 두 정책을 이중맹검 방식으로 쌍별 비교하여, 한 연구실의 고정 환경을 넘어서는 평가를 시도했습니다.

의미 수준의 안전도 별도 평가 축이 됩니다. 단순 충돌 여부가 아니라 위험한 명령을 거부하는지, 상황상 해서는 안 되는 행동을 구분하는지, 사람의 의도와 물리

적 결과가 충돌할 때 어떤 선택을 하는지를 봐야 합니다.

한 숫자에서 성능 프로필로

$$\text{평가} = \{\text{역량}, \text{강건성}, \text{복구}, \text{안전}, \text{불확실성 보정}, \text{평가 범위}\}$$

점수 하나가 아니라 배포 가능한 조건과 한계를 보여주는 성능 프로필이 필요합니다.

분산 평가가 드러내는 숨은 조건

이 다섯 변곡점 가운데 평가의 변화는 특히 확실한 흐름입니다. 범용 정책의 적용 범위가 넓을수록 개발팀이 고른 몇 가지 과업만으로는 주장을 검증하기 어렵습니다. 평가를 자동화하고 여러 장소로 분산하는 이유는 더 큰 숫자를 만들기 위해서가 아니라 **특정 장소와 개발팀의 설정에만 맞는 숨은 조건을 드러내기 위해서**입니다.

실패 분포까지 평가해야 한다

선별된 성공 영상과 소수 시험의 평균만으로는 범용 로봇을 평가할 수 없습니다. 여러 장소에서 반복 실행하고 실패 분포, 복구, 안전, 불확실성 보정까지 측정해야 합니다.

05. 안전하다는 주장보다 설계 단계의 입증 체계로

안전하다는 말과 안전의 증거는 다르다

안전이 위험을 줄이려는 목표라면, 안전성 입증은 어떤 위험을 분석했고 어떤 보호 장치가 실제로 작동하는지를 증거로 연결하는 일입니다. 모델 정확도를 높이는 것만으로 끝나지 않습니다.

안전성 입증 요소	확인할 증거
요구사항 추적	위험과 기능 요구가 설계·시험 항목으로 이어지는가
위험 분석	예상 가능한 위해와 심각도·발생 조건을 분석했는가
실행 중 통제	감시기, 속도·힘 제한, 독립 정지 기능이 작동하는가
인간 감독	사람이 언제 어떤 정보로 개입할 수 있는가
추적성	센서, 행동, 모델 버전, 상태가 기록되는가
변경 관리	업데이트 전후 회귀 시험과 되돌리기가 가능한가
생애주기 감시	배포 뒤 새로운 실패 유형을 수집·처리하는가

ISO 10218-1:2025는 산업용 로봇 자체의 안전 설계와 위험 저감을, ISO 10218-2:2025는 로봇을 응용 시스템과 작업 셀로 통합할 때의 안전 요구를 다룹니다. 이것은 AI 성공률이 높다는 주장과 실제 로봇 시스템의 안전 근거가 다른 차원임을 보여줍니다.

EU AI Act 는 모든 로봇을 자동으로 같은 위험 등급으로 지정하지 않습니다. AI 가 규제 대상 제품의 안전 구성요소인지, 해당 제품에 제 3 자 적합성 평가가 필요한지 등에 따라 분류와 요구사항이 달라집니다.

다수 조항은 2026 년 8 월 2 일부터 적용됩니다. 다만 로봇·산업기계 등 규제 제품에 내장된 고위험 AI 규칙은 2026 년 7 월 공표된 Regulation (EU) 2026/1744에 따라 2028 년 8 월 2 일부터 적용됩니다.

따라서 “2026 년에 모든 로봇 규제가 즉시 시작됐다” 고 단순화하면 안 됩니다. 중요한 방향은 위험 관리, 문서화, 인간 감독, 강건성, 모니터링이 제품 생애주기의 설계 변수로 들어온다는 점입니다.

업데이트 후 재검증 항목

새 정책이 기존 버전보다 성공률을 높였다고 합시다. 안전성 입증 관점에서는 다음 질문이 추가됩니다.

- 어느 조건에서 실패가 새로 생겼는가?
- 위험한 행동을 실행 전에 차단하는가?
- 사람이 언제 개입하고, 그 사건이 기록되는가?
- 기존 안전 요건이 업데이트 뒤에도 유지되는가?
- 일부 기체에서 제한 배포 시험을 거쳤는가?
- 문제가 생기면 로봇군 전체를 이전 버전으로 되돌릴 수 있는가?

성공률 개선은 시작점일 뿐, 변경된 시스템이 여전히 허용 가능한지 증거를 다시 만들어야 합니다.

표준과 규제의 적용 범위를 구분해야 한다

표준과 규제는 순수 알고리즘의 내부 변곡점이라기보다 연구를 실제 제품과 책임으로 연결하는 외부 조건의 변곡점에 가깝습니다. 적용 범위와 일정은 제품·용도·지역에 따라 다릅니다. 법률 자문 없이 특정 시스템의 규제 지위를 단정해서는 안 됩니다.

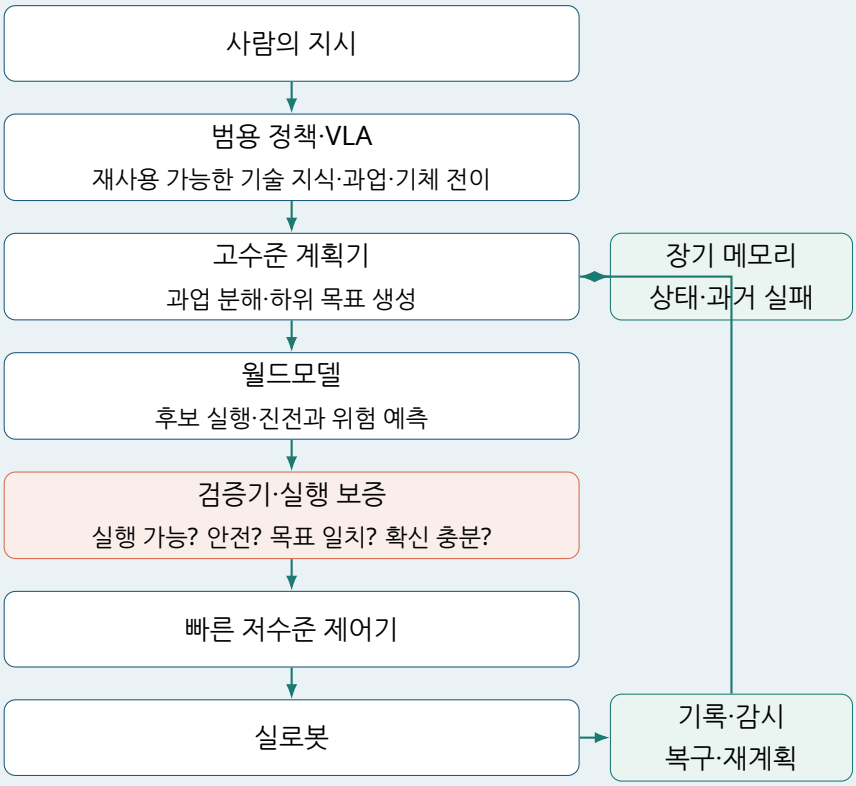
안전성은 작동 증거로 입증한다

"잘 작동했다" 만으로는 배포할 수 없습니다. 인간 개입, 로그, 강건성, 변경 관리, 사고 대응을 처음부터 시스템에 넣고 그 작동 증거를 남겨야 합니다.

다섯 변화를 하나의 로봇 시스템으로 연결하기

이제 다섯 변곡점을 한 시스템 위에 올려봅시다. 범용 정책은 여전히 중요하지만 전체 구조의 한 역할입니다.

다섯 변곡점을 연결한 Physical AI 실행 구조



새 조합을 해석하는 정책, 미래를 시험하는 월드모델, 상태를 유지하는 메모리, 실행을 승인하는 검증기, 실제 성능과 안전 근거를 기록하는 평가·입증 체계가 한 페루프를 이룹니다.

능력에서 책임까지

사전학습된 정책을 새 과업과 새 몸에 적은 비용으로 옮기는 일이 출발점입니다. 월드모델로 결과를 미리 시험하고, 메모리–계획기–제어기–검증기 구

조로 장기 실행의 실패를 관리해야 합니다. 이를 반복 가능한 실로봇 평가와 안전성 입증 체계로 검증하는 일이 2026 년 중순의 중심 과제로 올라왔습니다.

기술 발표를 평가하는 다섯 질문

1. 무엇이 실제로 처음 보는 과업 조합이며, 어느 기체까지 이전했는가?
2. 월드모델이 영상을 만들기만 했는가, 실제 페루프 결정을 개선했는가?
3. 누가 상태를 기억하고, 누가 행동을 승인하며, 실패하면 누가 복구하는가?
4. 몇 번·몇 장소·몇 기체에서 평가했고, 실패의 꼬리와 심각도는 어떠한가?
5. 모델이 바뀐 뒤에도 안전 주장을 지지하는 시험·로그·되돌리기 근거가 남는가?

핵심 개념 지도

핵심 용어를 시스템 역할별로 다시 정리합니다. 정의를 외우기보다 각 용어가 어느 입력을 받아 어떤 책임을 지는지 확인하십시오.

정책과 시간척도

Vision-Language-Action

시각과 언어를 행동으로 연결하는 범용 정책 계열이다. 핵심 가치는 자연어 인터페이스 자체보다 여러 작업과 기체에서 사전학습 자산을 재사용하는 데 있다. 저수준 제어와 안전 권한까지 하나의 모델에 맡길지, 전문 정책과 나눌지가 핵심 설계 질문이다.

정책 학습과 제어

표현 능력을 반복 가능한 물리 행동으로 바꾸는 마지막 계층이다. 의미 정책의 느린 주기와 서보 제어의 빠른 주기를 연결하며, 지연·진동·접촉 오차·외란을 다룬다.

확산·플로 매칭 (Diffusion·flow matching)

여러 형태의 연속 행동 분포를 보존하는 생성형 정책 방식이다. 평균화된 행동을 피하는 대신 반복 샘플링과 제어 지연이 생길 수 있어, 적은 단계의 생성·행동 묶음·가치 함수 유도가 중요하다.

계층적 구조

임무, 하위 목표, 기술, 모터 기본 동작을 서로 다른 시간척도로 나누는 설계다. 계산 절감뿐 아니라 실패 격리와 책임 추적을 가능하게 한다. 대신 계층 경계에서 정보 손실과 인터페이스 오류가 생길 수 있다.

폐루프

행동 결과를 재관측하고 다음 행동을 수정하는 조건이다. 특정 방법의 이름이라기보다 모든 정책이 실제 환경에서 통과해야 하는 평가 방식이다.

추가 학습 없는 추론 (Training-free inference)

가중치 업데이트 없이 검색, 일정 조정, 도구, 메모리, 후보 샘플링, 검증기로 행동을 개선한다. 버전 관리가 쉬울 수 있지만 계산량과 휴리스틱의 실패 위험은 남는다.

세계 상태와 감각

공간·기하 접지 (grounding)

언어와 픽셀을 실제 좌표, 방향, 도달 가능성, 충돌 여유로 고정하는 일이다. “무엇인가” 를 “어디를 어떻게 행동할 수 있는가” 로 바꾼다.

3D·BEV·LiDAR 인지

깊이, 자유 공간, 가림, 상대 속도를 계획기가 사용할 수 있는 상태로 만든다. 센서 보정과 동기화 비용이 크며, 명시적 상태와 잠재 표현 사이의 절충이 있다.

점유 표현 (Occupancy)

공간을 비어 있음, 점유됨, 알 수 없음으로 표현해 물체 종류와 무관하게 충돌과 이동 가능성을 다룬다. 의미·확률·시간 정보를 포함한 점유 표현으로 확장될수록 계획의 공유 상태가 된다.

의미 표현·의미 모델링

객체 이름을 기능, 행동 가능성, 역할, 관계, 과업 관련성으로 확장한다. 의미적 압축은 일반화를 돕지만 접촉과 정밀 기하를 잃지 않도록 해야 한다.

촉각·접촉·고유수용감각

시각으로 보기 어려운 미끄러짐, 힘, 삽입 상태, 관절 위치를 알려준다. 접촉 중심 조작의 핵심 피드백 경로지만, 센서별 차이와 시간 정렬이 어렵다.

멀티모달 학습

언어, 영상, 깊이, 촉각, 음향, 고유수용감각, 행동을 함께 다룬다. 감각 종류의 수보다 상황별 신뢰도에 따른 정보 선택, 결측 센서 강건성, 인과적 정렬이 중요하다.

SLAM·지도 구축

로봇의 위치와 환경 구조를 일관되게 유지한다. 장기 에이전트에서는 위치 추정 지도를 넘어 의미·작업 메모리의 좌표계가 되며, 갱신·망각·초기화 정책이 필요하다.

3D 가우시안 스플래팅

장면을 명시적인 3D 기본 요소들로 표현해 빠르게 렌더링하는 방식이다. 점진적으로 갱신되는 디지털 트윈과 센서 관측 변환에 유망하지만, 로봇용 지도가 되려면 동역학, 의미, 불확실성, 충돌 기하가 더 필요하다.

기억·추론·미래

메모리 (Memory)

현재 관측에 없는 진행 상태, 이전 행동, 가림 뒤 정보, 실패 경험을 보존한다. 저장량보다 검색, 갱신, 망각, 출처와 변경 이력이 중요하다.

추론

상황을 해석하고 도구, 제약, 중간 목표를 선택한다. 자연어 설명의 유창함이 아니라 실행 가능한 조건식, 좌표, 예상 결과와 모터 행동의 일치로 평가해야 한다.

계획

목표를 행동 순서와 궤적으로 바꾼다. 유연한 학습 기반 계획기와 보장성이 있는 기호·기하 제약을 짧은 구간마다 다시 계획하는 구조 안에서 결합하는 것이 현실적인 방향이다.

월드모델 (World model)

상태와 행동을 조건으로 미래 관측이나 상태를 예측한다. 렌더러, 시뮬레이터, 계획기의 역할을 구분해야 하며, 가치는 시각 품질보다 대안 행동 비교와 폐루프 성능 개선으로 입증해야 한다.

장기 작업

여러 단계의 누적 오류, 상태 망각, 단계 전환을 다룬다. 전체 성공률뿐 아니라 중간 상태 저장, 부분 완료, 작업 재개, 복구 시간이 핵심이다.

궤적·동작 예측

다른 행위자의 여러 가능한 미래를 예측한다. 자차의 행동에 따라 상대의 미래도 바뀌므로 여러 행위자의 상호작용과 대안 행동을 함께 표현한 분포, 불확실성 보정이 중요하다.

몸과 응용

체화형 AI(Embodied AI)

지식을 실제 감각, 행동, 결과 피드백에 접지하는 상위 문제다. 하나의 독립 알고리즘이라기보다 인지–추론–행동–검증으로 이어지는 전체 시스템을 가리킨다.

로봇 조작

VLA, 기하, 촉각, 계획, 복구를 함께 시험하는 대표 작업군이다. 단순 집기·놓기에서 도구 사용, 조립, 이동 조작, 가정 내 연속 작업으로 범위가 넓어진다.

정교 조작·양손·파지

작은 기하와 접촉 오차, 높은 자유도, 손 사이 상호작용을 다룬다. 과업 수준 정책과 빠른 손 제어기, 시각·촉각 피드백의 분업이 중요하다.

휴머노이드·다족 보행

이동과 조작이 결합된 전신 제어 문제다. 생성된 동작의 화려함보다 균형, 에너지, 낙상 복구, 사람 근접 안전, 시뮬레이션과 실세계의 차이를 봐야 한다.

항법

단순 목표점 도달에서 언어 목표, 의미 지도, 메모리, 사회적 상호작용, 조작 전환을 포함한 임무 수행으로 확장된다.

자율주행

대규모 센서 로그, 희귀 사건, 폐루프 시뮬레이션, 안전성 논증, 차량군 업데이트가 결합된 선행 응용이다. 학습된 핵심 모델과 명시적 안전 범위의 역할 분담이 중요하다.

UAV·공중 로봇

빠른 3D 동역학, 제한된 계산·배터리·통신, 추락 위험을 함께 가진다. 언어 기반 임무 계획기와 검증된 자동비행 제어기의 계층 결합이 현실적이다.

기체 간 전이 (Cross-embodiment transfer)

서로 다른 몸 사이에 과업 의미와 시각적 동역학을 공유한다. 공통 잠재 행동과 기체별 어댑터가 유망하지만 형태 차이에서 생기는 부정적 전이를 측정해야 한다.

다중 에이전트·협력

여러 로봇과 행위자가 역할, 지도, 메모리, 자원을 조정한다. 공유량보다 통신 단절, 분산 안전, 역할 충돌, 오류 확산을 다루는 통신·협력 규칙이 중요하다.

신뢰성·데이터·운영

강건성·일반화

환경 변화와 분포 이동에서 성능이 어떻게 무너지는지 다룬다. 변화 축을 분해하고 불확실성, 행동 보류, 분포 변화 탐지, 제한된 적응을 함께 평가한다.

효율화·압축

지연, 메모리, 에너지, 토큰, 샘플링 단계를 줄여 제어 주기와 엣지 자원 한도를 맞춘다. 모델 하나의 크기보다 센서–네트워크–하드웨어의 공동 설계가 중요하다.

벤치마크·평가

가능성을 검증 가능한 주장으로 바꾼다. 과업 성공 외에 장기성, 안전, 사람 개입, 복구, 처리량, 불확실성과 독립 평가 조건이 필요하다.

안전·위험

위험 인식뿐 아니라 행동 차단, 속도·힘 제한, 인간 개입, 사건 기록, 안전성 논증, 사후 모니터링을 포함하는 실행 보증 구조다.

실패 이해·복구·보정

실패를 탐지, 진단, 복구, 사람 이관으로 나눈다. 실패를 0 으로 만드는 것보다 복구 가능성과 평균 복구 시간이 운영가치를 좌우할 수 있다.

생성·시뮬레이션

실제 데이터가 부족한 희귀 상황과 대안 조건을 통제해 만든다. 시각 품질보다 물리·인과 타당성과 실제 정책 개선 효과를 검증해야 한다.

인간 선호·시연

정답 행동, 언어 교정, 결과 선호, 사람 개입을 통해 작업 기준을 전달한다. 신호마다 비용과 편향이 다르며 보상 지표의 편법 최적화와 평가자 간 불일치를 살펴야 한다.

무학습 일반화 (Zero-shot generalization)

추가 학습 데이터 없이 새로운 조건에 대응하는 능력이다. 물체, 장면, 과업 조합, 동역학, 센서, 기체를 구분하고 행동 거부와 복구까지 평가해야 한다.

데이터 수집·증강

실로봇 로그, 인간 영상, 합성 센서 데이터, 실패 이력을 연결한다. 양보다 품질 선별, 출처와 변경 이력, 이용 조건, 실패 범위, 실세계 재검증이 중요하다.

온라인 적응·지속 학습

배포 후 변한 환경에서 정책, 어댑터, 메모리, 기술을 갱신한다. 전체 모델 갱신보다 범위가 제한된 변경, 실제 실행 없이 이루어지는 그림자 평가, 버전 관리, 되돌리기가 현실적인 후보 패턴이다.

더 읽을 거리

아래 자료는 이 책의 기술적 배경과 공개 사례를 더 확인하기 위한 출발점이다. 기업 발표와 사전공개 논문의 결과는 해당 팀의 보고이며, 독립 재현이나 분야 전체의 보편적 성능을 뜻하지 않는다.

다섯 변곡점을 읽는 핵심 자료

CrossFormer: Scaling Cross-Embodied Learning

여러 로봇 기체의 데이터를 하나의 정책으로 학습해 기체 간 전이를 다룬 연구.

https://proceedings.mlr.press/v270/doshi25a.html

LAP: Language-Action Pre-Training

언어 형식의 저수준 행동 표현을 이용해 추가 학습 없이 기체 간 전이를 시도한 사전공개 연구.

https://arxiv.org/abs/2602.10556

DINO-WM

사전학습된 시각 특징의 미래를 예측하고, 목표 특징에 맞는 행동열을 최적화하는 계획 연구.

https://proceedings.mlr.press/v267/zhou25t.html

WorldGym (formerly Evaluating Robot Policies in a World Model)

행동 조건부 영상 모델에서 여러 번 가상 실행해 정책 순위를 추정하는 연구.

https://arxiv.org/abs/2506.00613

HAVE: History-Aware Verifier

행동 생성과 과거 상호작용을 이용한 후보 행동 검증을 분리한 연구.

https://proceedings.mlr.press/v305/li25e.html

HELM

장기 과업의 기억·검증·복구 격차를 모듈별로 분해한 사전공개 연구.

https://arxiv.org/abs/2604.18791

AutoEval

성공 판정과 장면 초기화를 자동화해 실제 로봇 정책을 반복 평가하는 연구.

https://arxiv.org/html/2503.24278v1

ISO 10218-1:2025

산업용 로봇 자체의 안전 설계와 위험 저감 요구사항.

https://www.iso.org/standard/73933.html

Navigating the AI Act

EU AI Act 의 분류와 요구사항을 설명하는 유럽연합 공식 안내.

https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act

본문의 공개 자료

π0.7: A Steerable Model with Emergent Capabilities

새 과업 조합, 기체 전이, 시각적 중간 목표를 포함한 범용 정책 사례.

https://www.pi.website/blog/pi07

Gemini Robotics-ER 1.6

공간 추론, 도구 호출, 물리적 제약을 다루는 체화형 추론 모델 사례.

https://deepmind.google/blog/gemini-robotics-er-1-6/

Cosmos 3

텍스트, 이미지, 영상, 음향, 행동과 정방향·역동역학을 함께 다루는 월드모델 연구.

https://research.nvidia.com/labs/cosmos-lab/cosmos3/

Vesta

위치 추정, 항법, 추론, 계획을 통합한 체화형 계획기.

https://research.nvidia.com/labs/gear/vesta/

Multi-Scale Embodied Memory

영상 단기 기억과 언어 장기 기억을 분리한 장기 로봇 작업 연구.

https://www.pi.website/research/memory

RL Token: Precise Manipulation with Efficient Online RL

가중치를 고정한 VLA 의 표현을 작은 행위자·평가기 모델의 현장 보정에 이용한 사례.

https://www.pi.website/research/rlt

ASPIRE

멀티모달 실행 기록, 반복 디버깅, 지속적으로 갱신되는 기술 라이브러리를 다룬 연구.

https://research.nvidia.com/labs/gear/aspire/

EgoScale

대규모 인간 1 인칭 영상과 정교 조작 전이를 다룬 연구.

https://research.nvidia.com/labs/gear/egoscale/

The Waymo World Model

희귀 주행 상황과 다중 센서 가상 실행을 생성하는 자율주행 월드모델 사례.

https://waymo.com/blog/2026/02/the-waymo-world-model-a-new-frontier-for-autonomous-driving-simulation/

Sensor2Sensor

외부 단안 영상을 다중 시점 카메라와 라이다 형식으로 변환하는 센서 시뮬레이션 연구.

https://waymo.com/research/sensor-2-sensor-cross-embodiment-sensor/

Waymo 6th-generation Driver

센서 수, 중복 구성, 전용 연산 장치의 시스템 공동 설계를 볼 수 있는 공개 자료.

https://waymo.com/blog/2026/02/ro-on-6th-gen-waymo-driver/

RoboArena

여러 기관의 실제 로봇을 이용한 분산·비교 평가 프로토콜.

https://robo-arena.github.io/

BEHAVIOR-1K

현실적인 장기 일상 작업과 전체 과업 평가를 다루는 벤치마크.

https://behavior.stanford.edu/index.html

VLA-Arena

안전, 교란 요소, 외삽 일반화, 장기 실행을 분리해 평가하는 환경.

https://vla-arena.github.io/

ISO 10218-2:2025

산업용 로봇 응용 시스템과 작업 셀의 통합·운영·유지보수에 관한 안전 요구.

https://www.iso.org/standard/73934.html

EU AI Act official timeline

2026 년 7 월 24 일 갱신된 유럽연합 공식 적용 일정. 규제 제품에 내장된 고위험 AI 규칙은 2028 년 8 월 2 일부터 적용된다고 설명한다.

https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Regulation (EU) 2026/1744

EU AI Act 의 적용 일정을 개정한 2026 년 7 월 공표 규정 원문.

https://eur-lex.europa.eu/eli/reg/2026/1744/oj

Do What You Say

언어 계획과 모터 행동의 불일치를 실행 중 추론과 검증으로 다룬 연구.

https://research.nvidia.com/publication/2026-06_do-what-you-say-steering-vision-language-action-models-runtime-reasoning-action

FAST

연속 로봇 행동을 압축하는 행동 토큰화 연구.

https://www.pi.website/research/fast

Real-Time Action Chunking

대형 정책의 추론 중에도 계속 변하는 세계에서 비동기 행동을 연결하는 방법.

https://www.pi.website/research/real_time_chunking

Gemini Robotics On-Device

낮은 지연과 네트워크 독립 실행을 겨냥한 기기 내 로봇 모델 사례.

https://deepmind.google/blog/gemini-robotics-on-device-brings-ai-to-local-robotic-devices/

Sparsh

대규모 자기지도 촉각 표현과 여러 촉각 센서·과업을 다룬 연구.

https://ai.meta.com/research/publications/sparsh-self-supervised-touch-representations-for-vision-based-tactile-sensing/

Diffusion Policy

여러 봉우리를 가진 연속 행동 분포와 이동 지평 제어에 확산 모델을 적용한 기초 연구.

https://diffusion-policy.cs.columbia.edu/

Spark 2.0

대규모 3D 가우시안 스플래팅 세계의 스트리밍과 세부 수준 조절 사례.

https://www.worldlabs.ai/blog/spark-2.0

LoopSplat

3D 가우시안 부분 지도의 온라인 루프 폐쇄와 전역 일관성을 다룬 연구.

https://www.research-collection.ethz.ch/items/1a129549-57a5-4cb7-abcc-148920c202c1

Uni-LaViRA

여러 항법 과업과 기체를 하나의 에이전트 실행 루프로 다루는 사전공개 연구.

https://arxiv.org/abs/2605.27582

WorldFly

도시 환경 UAV 에서 미래 영상과 행동을 함께 생성하는 사전공개 연구.

https://arxiv.org/abs/2606.06147

GR00T N1.6

여러 로봇 기체의 양손 조작과 이동·조작 통합을 다루는 공개 모델 자료.

https://research.nvidia.com/labs/gear/gr00t-n1_6/

GRAIL

3D 자산과 영상 사전지식으로 전신 동작열을 생성하고 실기체로 옮기는 연구.

https://research.nvidia.com/labs/dair/grail/

Open X-Embodiment

여러 기체의 로봇 궤적을 모은 초기 대규모 데이터 협력.

https://robotics-transformer-x.github.io/

Hi Robot

고수준 VLM 과 저수준 VLA, 사람의 중간 개입을 결합한 계층형 정책.

https://www.pi.website/research/hirobot

AutoRT

여러 로봇의 대규모 데이터 수집과 로봇군 임무 조정을 다룬 연구.

https://deepmind.google/research/publications/48151/

GenDP

3D 의미장과 확산 정책을 결합해 보지 못한 개체를 조작하는 연구.

https://robopil.github.io/GenDP/

UniScene

의미 점유 표현을 중심으로 영상과 라이다 생성을 통합한 주행 장면 생성 체계.

https://cvpr.thecvf.com/virtual/2025/poster/32687

A Functional Taxonomy of World Models

렌더러, 시뮬레이터, 계획기와 그 사이의 실행 루프를 구분하는 개념 틀. 합의된 표준 정의라기보다 유용한 분석 관점으로 읽는다.

https://www.worldlabs.ai/blog/taxonomy-of-world-models

2026 하반기 Physical AI 동향

이 책은 2026 년 7 월 26 일까지 공개적으로 확인할 수 있는 자료를 바탕으로 한다.

이후 전망은 관찰 지표와 반증 조건에 따라 달라질 수 있으며, 안전·규정·제품 판단은 용도별 검증이 필요하다.