설계 엔지니어링을 위한
AI 도입 가이드라인



kenca 한국엔지니어링협회
KOREA ENGINEERING & CONSULTING ASSOCIATION

BIM 한국BIM학회
Korean Institute of Building Information Modeling

CONTENTS

1 비전 수립 및 단계별 전략 1
1.1 배경 및 필요성 1
1.2 AI 도입 전략 2

2 조직 운영 및 인력 전략 4
2.1 배경 및 필요성 4
2.2 조직 운영 및 인력 전략 4

3 교육 및 역량 강화 7
3.1 배경 및 필요성 7
3.2 교육 및 역량 강화 전략 7

4 범용 AI 서비스 활용 및 보안 관리 10
4.1 배경 및 필요성 10
4.2 범용 AI 활용 전략 11
4.3 보안 전략 12

5 성과품 데이터화 및 중앙 관리 15
5.1 배경 및 필요성 15
5.2 AI를 위한 데이터화 전략 16
5.3 AI 분석에 적합한 데이터 형식 17
5.4 PDF와 Markdown 형식의 최적 조합 전략 19

6 제언 20
6.1 설계사 규모별 맞춤 전략의 필요성 20
6.2 중소 설계사 전략 20
6.3 중대형 설계사 전략 20
6.4 대형 설계사 전략 21

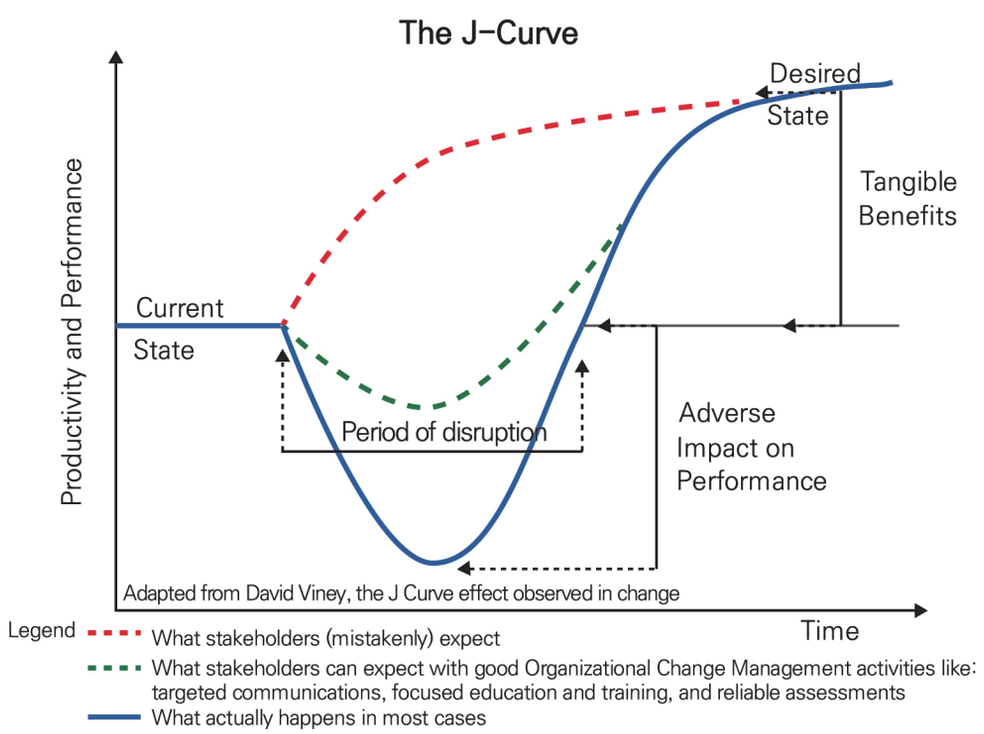
1 비전 수립 및 단계별 전략

1.1 배경 및 필요성

① AI 도입 전략 부재

- AX(AI Transformation)·DX(Digital Transformation)가 장기적으로 설계 업무의 생산성과 품질의 향상 측면에서 실질적인 성과를 내기 위해서는 기업은 물론이고 국가적으로도 AI 도입에 대한 구체적이고 체계적인 전략을 세워야 한다.
- 단기적 성과와 단순한 형태의 도구 활용 정도의 답습에 의존하게 되면, 오히려 설계 업무 효율 측면에서 역효과가 발생할 수 있고, 결과적으로 AX·DX가 초기의 혼란기(Period of Disruption)에서 멈춰버리고, 투자 대비 효과를 보지 못한 채 중단될 수 있다.

그림 1 브린욜프슨의 ICT 생산성 J커브



Aspects of J-curve of change.

출처: https://spri.kr/posts/view/23483?code=data_all&study_type=&board_type=issue_reports

② 국가 정책 및 발주처 로드맵과의 연계성 확보

- 더욱이 건설 설계 산업의 디지털 전환과 AI 도입은 정부 정책 및 발주처의 로드맵과 직결되어 있다.
- BIM(Building Information Modeling) 의무화, 스마트 건설 기술 도입, 공공부문 초거대 AI 활용 지침 등을 지속적으로 추진하는 국토교통부와 주요 발주처들의 움직임에 맞추어 설계사에서도 내부 전략을 수립하여야 향후 공공 프로젝트 수주 경쟁력을 유지하거나 제고할 수 있다.

1.2 AI 도입 전략

① 1단계 : 정량 목표를 포함한 'AI·DX·AX 비전' 문서화

- AI 도입의 비전을 추상적인 구호가 아닌 구체적이고 측정 가능한 목표로 제시한다.

표 1 정량적 목표 예시

- "3년 내 설계 문서 작성 및 검토 시간 20% 절감"
- "품질 관련 클레임 발생률 30% 감소"
- "설계 기준 및 법령 검색 소요 시간 50% 단축"

- 추상적인 "디지털 혁신"보다는 구체적인 숫자로 표현된 목표가 실무자들에게 훨씬 명확한 방향성을 제공한다.
- 이러한 정량적 목표를 **사내 공식 문서**로 선언하고, 경영회의와 직원 교육에서 반복적으로 언급하여 조직 전체가 공통된 목표를 지향해야 한다.

② 2단계 : 중장기(5년) AI·DX·AX 로드맵 수립

- 정부 및 주요 발주처의 디지털 로드맵을 면밀히 분석하여, 자사의 중장기 로드맵을 체계적으로 구성한다.

표 2 중장기 로드맵 예시

- **1단계(1~2년차): 반복 업무 자동화**
  문서 작성, 기준 검색, 품질 체크리스트 검토 등 반복적이고 규칙적인 업무에 AI를 적용한다. 이 단계에서는 빠른 성과 창출과 조직의 AI 익숙화가 목표이다.
- **2단계(2~3년차): 설계 프로세스 내 AI 표준 프로세스 도입**
  1단계에서 검증된 AI 활용 방법을 설계 프로세스의 표준으로 정립한다. 예를 들어 "보고서 작성 시 반드시 AI 초안 작성 → 실무자 검토 → 최종 승인" 같은 표준 절차를 수립한다.
- **3단계(4~5년차): 사내 LLM/RAG 플랫폼 및 에이전트 체계 구축**
  외부 범용 AI 서비스에만 의존하지 않고, 회사의 고유 데이터와 노하우가 결합된 자체 AI 플랫폼을 구축한다. 이를 통해 경쟁사와 차별화된 설계 역량을 확보할 수 있다.

③ 3단계 : 연 1회 AI·DX·AX 수준 자체 평가

- 매년 정기적으로 자사의 디지털 전환 및 AI 전환 수준을 평가하는 체크리스트를 마련하고 운영한다.

표 3 AI·DX·AX 수준 평가 체크리스트 예시

- **AI 활용도**
  - 몇 개 업무 영역에서 AI를 활용하는가?
  - 전체 임직원 중 몇 %가 정기적으로 AI를 사용하는가?
- **데이터 관리 수준**
  - 성과품과 내부 문서가 표준화되어 있는가?
  - 중앙 집중식으로 관리되는가?
  - 데이터 정제 작업이 체계적으로 이루어지는가?
- **자동화 수준**
  - Dynamo 및 GC 등을 활용하여 업무 자동화하고 있는가?
  - RPA(로봇 프로세스 자동화)를 활용하여 업무를 자동화하고 있는가?
  - BIM과 수량산출 및 내역서의 자동 연동이 어느 수준까지 구현되어 있는가?

- 매년 평가 결과를 경영진과 전 직원에게 공유하고, 이를 바탕으로 다음 연도의 로드맵을 조정함으로써 지속적인 개선의 동력을 제공한다.

④ 4단계 : '작은 성공' 중심의 단계적 확산 전략

- "작은 성공의 축적"을 통한 점진적 AI 도입 전략을 수립한다. (조직 구성원의 충분한 학습 및 적응 기간 확보로 장기적으로 실질적 효과 달성)

표 4 단계적 확산 전략 예시

- **선택과 집중**
  전체 부서가 아닌 1~2개 부서, 전체 업무가 아닌 1~2개 업무를 신중하게 선정한다.
- **파일럿 운영**
  선정된 영역에서 3~6개월간 파일럿 프로젝트를 운영한다.
- **검증 및 보완**
  파일럿 결과를 면밀히 분석하고, 문제점을 보완한다.
- **수평 확산**
  검증된 방법론을 다른 부서와 업무 영역으로 점진적으로 확산시킨다.

- "한 번에 전사에 도입하려는 시도"는 오히려 역효과를 일으키고 성공적 도입을 저해할 수 있으므로 지양한다.

2 조직 운영 및 인력 전략

2.1 배경 및 필요성

① 전담 조직 부재

- 장기적인 AI 전략을 지속적으로 추진하기 위해서는 기업 차원의 AI 전담 조직 구성이 필수적이다.

② 부서 사일로(Silo) 구조의 한계

- 도로부, 교량부, 구조부, 지반부 등이 독립적으로 운영되고 있는 대부분 설계사의 부서 사일로(Silo) 구조 환경에서는 다음과 같은 문제가 발생할 수 있다.

표 5 건설 조직의 문제

- **데이터 중복 및 누락**
  동일한 프로젝트가 부서별로 따로 관리되어 데이터 중복 생성 또는 데이터 누락의 문제 발생
- **데이터 충돌**
  각 부서가 서로 다른 형식과 기준으로 데이터를 관리하여, 데이터 통합 시에 충돌 발생
- **체계적 AI 데이터 구축 불가**
  부서 사일로 환경에서는 AI 학습 및 활용을 위한 체계적인 데이터베이스 구축 불가능

③ 새로운 조직 구조의 필요성

- AI와 BIM을 효과적으로 활용하려면 프로젝트 전 과정을 관통하는 일관된 데이터 흐름이 필요하고, 이를 위해서는 보고서 작성, 수량 산출, 협의 자료 준비 같은 공통 Back-office 업무를 전담하는 조직 확보가 필수적이다.

2.2 조직 운영 및 인력 전략

① 1단계 : 실무 중심 '경량 AI TF' 구성

- AI 도입을 위한 전사적인 대규모 조직 개편을 추진하기에 앞서, 먼저 실무 중심의 경량 AI TF(Task Force)를 구성한다.
- 구성 방식은 각 부서에서 파견된 실무자(각 1~2명) + 기술연구소 인원으로 총 5~10명 규모로 시작하되, "형식적 TF"가 아니라 "실제로 움직이는 실무 조직"으로서 명확한 목표를 설정한다.
- TF는 "AI 전문가 집단"이 아니라 "AI를 실무에 적용하는 방법을 함께 찾아가는 실무자 집단"으로 운영한다.

표 6 실무 중심의 경량 AI TF팀의 역할

- 현장에서 발생하는 AI 활용 아이디어를 수집하고 정리
- PoC(Proof of Concept: 개념 검증) 과제를 선정하고 직접 추진
- 사내 AI 활용 가이드, 템플릿, 프롬프트 라이브러리를 작성하고 공유
- 경영진의 전략적 요구와 현장의 실무적 요구를 중간에서 조율

② 2단계 : 신입·초급 엔지니어를 '데이터 구축 핵심 인력'으로 활용

- 장기적 관점에서 신입사원과 초급 엔지니어를 데이터 구축의 핵심 인력으로 활용하는 것이 중요하다.
- 신입사원 입사 후 6개월~1년간 다음 업무를 집중적으로 수행하게 한다.

표 7 입사 초기 업무 예시

- 과거 성과품의 디지털화 작업 (스캔 문서를 검색 가능한 텍스트로 변환)
- 문서에 메타데이터 부여 및 태깅 작업 (프로젝트명, 날짜, 분야, 키워드 등)
- 설계 기준 및 지침을 항목 단위로 분할(Chunking)하는 작업

- 이러한 전략을 통해 다음의 두 가지 이점을 얻을 수 있다.
  - 신입사원 관점 : 회사의 과거 프로젝트를 검토하면서 실무를 이해하고 학습
  - 회사 관점 : AI 활용을 위한 고품질 데이터베이스를 체계적으로 구축

③ 3단계: 전사 차원 Back-office형 조직 운영

- 기존의 부서 사일로 구조를 개선하기 위해 장기적으로 다음과 같은 조직 운영을 검토한다.
- 통합 조직 구성
  - 건설 설계 업무의 일반적 절차인 '조사 → 계획 → 기본설계 → 실시설계 → 성과품 작성 → 발주처 협의' 중, '조사', '성과품 작성', '발주처 협의 자료 준비' 등의 업무는 부서별 수행이 아니라 전사적 차원의 업무 수행이 가능하도록 별도 조직을 구성하는 것이 효율적이다.

표 8 통합 조직의 역할

- **프로젝트 초기 조사팀**
  모든 부서의 현장 조사, 문헌 조사, 기초 데이터 수집을 통합 수행
- **성과품 작성팀**
  최종 보고서, 도면 정리, 수량 산출서 등을 전문적으로 작성
- **협의 자료팀**
  발주처 제출 자료, 협의 자료를 통합 관리

- BIM 통합 관리 조직 구성
  - BIM 업무는 부서별로 서로 다른 특화 프로그램을 사용하면 최종 단계에서 이들을 통합할 때 데이터 충돌과 수정의 어려움이 발생할 수 있으므로, 전사 차원의 BIM 표준을 수립하고 BIM 데이터를 통합 관리하는 전담 조직이 필요하다.
- 신입사원 배치 전략
  - 신입사원이나 초급 기술자를 처음부터 "도로", "구조", "지반", "수자원" 등으로 세분화하여 배치하지 않고, 다음과 같은 범용 업무를 전반적으로 수행하게 하는 것이 효율적이다.
  - 이를 통해 초급 기술자가 엔지니어링 업무 전반에서 AI와 BIM을 활용하는 경험을 습득하고, 추후 중급 및 고급 기술자로 성장했을 때 더 넓은 범위에서 이러한 기술을 활용할 수 있는 역량을 갖출 수 있다.

표 9 신입사원을 위한 범용 업무 예시

- 보고서 최종 수정 및 편집
- 성과품 상세 내용 수정
- 수량 집계 및 확인
- 구조계산서 산출물 정리
- 협의용 자료 수집 및 정리

④ 4단계: 조직의 자발적 참여 유도

- 조직의 자발적 참여를 유도하기 위하여 포상 제도를 마련한다.

표 10 조직의 자발적 참여 유도 예시

- **아이디어 수집**
  "AI로 이런 업무를 자동화해봤다", "이런 프롬프트를 만들어서 업무 시간을 줄였다"는 등의 실제 사례를 정기적으로 수집하고 사내에 공유
- **AI 활용 경진대회**
  연 1회 'AI 활용 우수 사례 경진대회'를 개최하여 우수 사례를 발굴하고 포상 (금전적 보상 외에 승진 심사나 인사 평가에 반영하여 높은 참여율 유도)

3 교육 및 역량 강화

3.1 배경 및 필요성

- Upskilling(기존 역량 향상)과 Reskilling(새로운 역량 습득)
  - "소수의 AI 전문가"보다 "모든 직원의 AI 활용 능력 향상"에 초점을 둬야 한다.
    (AI 도입 성공 사례의 공통된 요인)
- 지속적인 사례 중심의 교육을 통한 설계 실무자의 AI 역량 강화 전략이 필요하다.
  - 일회성 특강 또는 외부강사 이론 교육만으로는 실질적 역량 강화 기대하기 어렵다.
  - 실무자 간 일원화된 방식의 AI 활용이 이뤄지도록 교육을 마련해야 한다.

표 11 AI 활용 시 주요 위험 요소

- **환각(Hallucination)**
  AI가 그럴듯하지만 틀린 정보를 제공하는 현상
- **보안 사고**
  민감한 정보를 부주의하게 AI에 입력하여 유출되는 사고
- **잘못된 의존**
  AI 결과를 검증 없이 그대로 사용하는 문제

3.2 교육 및 역량 강화 전략

① 1단계 : 월 1회 '실무사례 중심 AI 워크숍'

- 단순한 AI 이론 교육이 아닌, 실제 업무에서 AI를 활용한 사례를 중심으로 한 워크숍을 정기적으로 운영한다.

표 12 워크숍 구성 요소 예시

- **성공 사례 공유**
  실제 설계 업무에서 AI를 활용하여 업무 시간을 단축하거나 품질을 향상시킨 사례를 공유 (예: "보고서 초안 작성에 AI를 활용하여 3시간 작업을 30분으로 단축")

- **성공 사례 공유**
  실제 설계 업무에서 AI를 활용하여 업무 시간을 단축하거나 품질을 향상시킨 사례를 공유 (예: “보고서 초안 작성에 AI를 활용하여 3시간 작업을 30분으로 단축”)
- **실패 사례 공유**
  실패 사례 또한 재발하지 않도록 중요한 교육자료로 공유 (예: “AI가 생성한 설계 기준 조항이 틀렸는데 확인하지 않고 사용한 사례”, “보안이 필요한 프로젝트 정보를 AI에 입력한 사례”)
- **베스트 프롬프트 공유**
  매달 가장 효과적이었던 프롬프트(AI에게 주는 지시문)를 선정하여 공유 (예: “구조계산서 결과를 표로 정리하는 프롬프트”, “설계 기준 조항을 요약하는 프롬프트” 등)

- 발표자는 외부 강사보다 내부 실무자를 우선적으로 선정한다.
  - 같은 실무자가 발표할 때 참석자들의 공감도와 학습 효과가 훨씬 높다.

② 2단계 : 직급·역할별 맞춤형 교육 체계

- 모든 직원에게 동일한 교육을 제공하기보다 직급과 역할에 따라 차별화된 교육을 제공하는 것이 효율적이다.

표 13 맞춤형 교육 내용 예시

- **주니어(신입~3년차) 대상 교육**
  - 범용 AI의 기본 사용법 (ChatGPT, Claude 등의 기본 사용)
  - 효과적인 프롬프트 작성 방법
  - 문서 요약, 번역, 보고서 초안 작성 등 기본 활용법
  - 사내 RAG 검색 시스템 활용법
  - 보안 수칙 (어떤 정보를 AI에 입력하면 안 되는지에 대한 명확한 가이드)
- **미들(4~10년차) 대상 교육**
  - 품질 검토 자동화 방법
  - 설계 기준 및 코드 자동 체크 시스템 활용
  - 설계 파라미터 추천 시스템 활용
  - AI 결과물의 검증 방법
  - 복잡한 프롬프트 엔지니어링 기법
- **시니어·관리자(10년차 이상) 대상 교육**
  - AI 도입 전략 및 ROI(투자 대비 효과) 계산
  - AI 관련 리스크 관리 (법적, 윤리적, 보안 측면)
  - 팀 단위 AI 도입 및 조직 운영 방법
  - 발주처의 AI 요구사항 이해 및 대응 전략

③ 3단계 : LLM/RAG 집중 교육

- 기술적으로 한 단계 더 깊이 있는 이해가 필요한 인력을 위해 전문 교육을 제공한다.
- 교육 주기는 분기 1회(3개월마다) 정도 진행하며, 사내 전문가 또는 외부 컨설턴트와 함께 실습 위주로 운영한다.

표 14 집중 교육 내용 예시

- **RAG(검색-증강-생성) 개념**
  단순 LLM 대비 RAG 도입의 장점
- **건설/설계 분야 적용 사례**
  국내외 선진 사례 분석
- **벡터DB의 이해**
  문서가 벡터 데이터로 변환되는 개념
- **Chunking 전략**
  설계 기준 문서를 의미 단위로 나누는 기준
- **프롬프트 설계 실습**
  실제 설계 업무에 적용 가능한 프롬프트를 직접 작성하고 테스트

4 범용 AI 서비스 활용 및 보안 관리

4.1 배경 및 필요성

① 범용 AI 활용 전략 필요성

- 중소 규모 설계사가 보안 문제 해결을 위해서 자체 AI를 개발하는 것은 비효율적일 수 있으며, 상대적으로 범용 AI를 안전하게 활용하는 방법을 확립하는 것이 효율적이다.

② 기업별 보안 수준의 편차

- 보안관리 수준은 설계사에 따라 편차가 큰 편이며, 이는 상당수의 설계사가 보안 사고 위험에 노출되고 있음을 의미한다.
- 보안 사고가 한 번 발생하면 회사의 신뢰도에 치명적인 타격을 입을 수 있다.

표 15 보안 수준 인터뷰 내용

- “특별한 보안 규정이 거의 없고, 개인 판단에 맡긴다”
- “프로젝트별 보안 등급을 설정하고, 민감 키워드 차단 시스템을 운영한다”

③ 공공부문 AI 가이드의 요구사항

- 공공부문 초거대 AI 도입 가이드의 필수 요소와 함께, 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」(제31조 인공지능 투명성 확보 의무)에서 규정하는 법적 의무 사항을 선제적으로 반영한다.
- 보다 상세한 보안 기준 및 실무 적용 방법은「국가 공공기관 AI 보안 가이드북(안전한 AI시스템 도입·활용을 위한 보안 안내서)」, 「인공지능 투명성 확보 가이드라인」「인공지능(AI) 보안 안내서」등을 참조한다.

표 16 공공부문 AI 도입 시 사전 고려 사항

- **생성형 인공지능이 가져올 위험을 이해하고 방지**
  - 조직 내외의 민감정보, 개인정보 보호 대책 강구
  - 인공지능의 윤리성 확보를 위한 기술적, 제도적 조치 강구
- **데이터의 보안등급에 따른 보안대책 마련**
  - 업무 중요도에 따라 기밀(Classified), 민감(Sensitive), 공개(Open) 등 3개 등급으로 분류하여 보안정책 적용

4.2 범용 AI 활용 전략

① 업무용 계정 기반의 구독·지원 체계 구축

- ChatGPT, Claude, Gemini 등 범용 AI는 회사가 업무용 계정(개인형·부서공유형)을 선정·구매하여 공식 채널로 사용하도록 제공한다.
- 직무별·활용 수준별로 권한과 사용 범위를 나누어, 과도한 비용·무분별한 사용을 동시에 통제한다.

② 업무 유형별 활용·금지 영역 구분

- 아이디어 브레인스토밍, 문서 초안·요약·번역, 코드·스크립트 작성 보조 등 비(非)민감·내부 참고용 업무는 범용 AI 활용을 적극 권장한다.
- 발주처·계약정보, 상세 도면·수량·단가 등 민감 데이터가 포함되는 업무는 범용 AI 입력을 원칙적으로 금지하고, 자체 시스템·내부 전용 AI로만 처리하도록 규정한다.

③ 범용 LLM + 사내 RAG 결합 구조 채택

- 질의·텍스트 생성은 범용 LLM의 장점을 활용하되, 설계 기준·시방서·성과품 등 내부 문서는 사내 RAG(벡터DB 기반 검색 시스템)를 통해서만 참조하도록 구조를 설계한다.
- 즉, LLM은 밖의 것, 데이터는 안의 것이라는 원칙으로, 범용 AI의 성능과 사내 데이터 보안을 동시에 확보한다.

④ 검증·승인 절차를 거친 결과만 성과품에 반영

- 범용 AI가 생성한 문서·표·설계 설명 등은 반드시 담당 엔지니어의 검토·수정·승인을 거친 후에만 성과품·대외 문서에 반영한다.
- AI 결과물은 “초안/보조도구”로 명시하고, 최종 책임은 항상 담당 기술자에게 있다는 원칙을 내부 규정에 포함한다.
- 해당 결과물을 발주처 제출용 대외 문서에 반영하는 경우, 문서 내 AI 생성 사실을 표시하여 「인공지능기본법」상 투명성 확보 의무(4.3 6단계 참조)를 준수한다.

⑤ 사용 로그·사례 기반 지속 개선

- 범용 AI 사용 이력·사례를 정기적으로 수집·분석하여, 잘 쓰인 예시와 문제 사례(환각·보안 위험)를 교육 자료로 재활용한다.
- 이를 바탕으로 프롬프트 가이드, 금칙어 목록, 활용·금지 예시를 주기적으로 업데이트하여 전사 활용 수준을 단계적으로 높인다.

4.3 보안 전략

① 1단계 : 데이터 보안 등급 분류(C/S/O) 도입

- “공공부문 초거대 AI 도입·활용 가이드라인”에서 제시하고 있는 데이터 보안 등급을 활용하여 모든 데이터를 세 가지 등급으로 명확히 분류한다.
- 각 프로젝트 시작 시 문서의 보안 등급을 명확히 지정하고, 파일명이나 메타데이터에 등급을 표시하여 실수를 방지한다.

표 17 주요 문서별 데이터 보안 등급 예시

	C등급 (기밀, Confidential)	S등급 (민감, Sensitive)	O등급 (공개, Open)
대상 자료	발주처와의 계약서, 협약서, 미공개 입찰 제안서, 상세 도면 원본, 프로젝트 금액, 단가 정보	발주처명이 포함된 문서, 프로젝트 위치 정보, 주민번호, 법인번호, 내부 회의록 등 민감 내용	홍보 자료, 공개된 보고서, 일반적인 설계 기준(공개 문서), 사내 교육 자료
활용 여부	**AI 입력 금지**	**AI 입력 시 사전 승인 필요**	**사전 승인 필요 없음**

② 2단계 : ‘무조건 업로드 금지’ 영역 명문화

- 보안 등급 체계와 별도로, 어떤 상황에서도 범용 AI에 입력해서는 안 되는 항목을 사규 또는 가이드로 명시한다.
- 이를 사내 게시판, 교육 자료, 업무 매뉴얼에 반복적으로 공지하고, 위반 시 인사 규정에 따라 처리한다는 점을 명시한다.

표 18 업로드 금지 항목 예시

- 발주처 계약서·협약서 전문
- 미공개 입찰 제안서의 핵심 내용
- 상세 도면 원본 파일
- 민감한 수량·단가·공사비 정보
- 주민번호, 법인번호 등 개인정보
- 내부 인사 정보

③ 3단계 : 범용 AI 접근 통제 및 키워드 필터링

- 기술적으로 가능하다면, 다음과 같은 통제 시스템을 구축한다.
  - 이는 직원의 부주의나 실수로 인한 정보 유출을 기술적으로 방지하는 최종 방어선으로, 교육만으로는 완전히 제어하기 어려운 휴먼 에러를 시스템적으로 보완하는 역할을 한다.

표 19 통제 시스템 예시

- **네트워크 레벨 모니터링**
  내부망에서 외부 AI 서비스(ChatGPT, Claude 등)로 나가는 트래픽을 모니터링합니다.
- **키워드 필터링 시스템**
  다음과 같은 민감 키워드가 포함된 텍스트가 AI 서비스로 전송되려 할 때 경고 또는 차단합니다.
  - 회사의 프로젝트 코드 (예: PRJ-2024-001)
  - 주요 발주처명 (예: 국토교통부, 한국도로공사)
  - 주민번호, 사업자번호 패턴
  - "입찰", "계약금액" 등 민감 용어

④ 4단계 : 글로벌 SaaS AI 사용 시 '학습 비활성화(Opt-out)' 적용

- Autodesk, Microsoft Copilot 등 글로벌 SaaS(클라우드 기반 소프트웨어) AI 서비스를 사용할 때는 다음 사항을 반드시 확인한다.
  - 대부분의 상용 AI 서비스는 사용자가 입력한 데이터를 향후 모델 학습에 사용할 수 있게 되어 있으나, 유료 서비스인 경우 학습 비활성화(Opt-out) 옵션을 통해 사용자 데이터가 모델 학습에 사용되지 않도록 설정할 수 있다.

⑤ 5단계 : LLM은 범용, 데이터는 사내 RAG 구조로 분리

- 가장 현실적이고 효과적인 보안 전략은 하이브리드 구조이다.
- 하이브리드 구조 설계 원칙
  - LLM(언어 모델) : ChatGPT, Claude 등 범용 AI 서비스 활용
  - 데이터(지식 베이스) : 설계 기준, 성과품, 내부 매뉴얼 등은 사내 RAG 서버 + 벡터DB에만 저장

표 20 하이브리드 작동 방식 및 장점

- **작동방식**
  1. 사용자가 "OO 교량 설계 기준 3.2조항이 뭐야?"라고 질문
  2. 질문은 먼저 사내 RAG 서버로 전송
  3. RAG 서버가 사내 벡터DB에서 관련 설계 기준 조항 검색
  4. 검색된 조항만 범용 LLM에 전달
  5. LLM이 검색 결과를 바탕으로 답변을 생성하여 사용자에게 제공
- **장점**
  - 보안 : 민감한 전체 데이터베이스는 외부로 나가지 않고, 필요한 부분만 일시적으로 전달
  - 성능 : 최신 범용 LLM의 우수한 언어 이해 및 생성 능력 활용
  - 비용 : 자체 LLM 개발/운영 비용 절감
  - 유지보수: 설계 기준 변경 시 사내 DB만 업데이트하면 즉시 반영

⑥ 6단계 : AI 생성물 투명성 확보 및 표시 원칙 수립

- 2026년 1월 22일 시행되는 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 제31조(인공지능 투명성 확보 의무)에 따라, 고영향 인공지능 또는 생성형 인공지능을 이용한 제품·서비스를 제공하는 경우 해당 사실을 사전에 고지하고, 그 결과물이 인공지능에 의해 생성되었음을 표시하여야 한다.
- 회사가 발주처에 제출하는 보고서, 도면, 협의자료 등 대외 성과품에 범용 AI를 활용하여 초안을 작성하거나 보조적으로 활용한 경우, 해당 사실을 문서 표지·머리말 또는 파일 메타데이터에 명시하는 사내 표준 절차를 마련한다.

표 21 AI 생성물 표시 방법 예시

구분	예시
문서형 성과품 (보고서, PDF, 워드)	머리말 또는 표지 하단에 “본 문서의 일부는 생성형 인공지능을 활용하여 작성되었으며, 담당 기술자의 검토·승인을 거쳤습니다.” 문구 표시
이미지·도면·조감도·시뮬레이션 영상	파일 메타데이터 또는 도면 우측 하단에 AI 활용 사실 기록. 실제와 구분하기 어려운 시뮬레이션 영상·조감도는 일반 생성물보다 명확한 표시 방법(가시적 워터마크 등)을 적용
사내 전용 자료	사전 승인 절차를 거쳐 내부용으로만 사용하는 경우 표시 생략 가능. 단, 발주처 제출 등 대외 반출 시에는 반드시 표시

5 성과품 데이터화 및 중앙 관리

5.1 배경 및 필요성

① 전통적 파일 관리의 한계

• 현재 다수의 설계사가 웹하드, NAS(Network Attached Storage) 등 전통적인 파일 서버에 프로젝트별 폴더 구조로만 문서를 관리하고 있으나, 이러한 방식은 다음과 같은 심각한 한계를 가지고 있다.

표 22 전통적 파일 관리 방식의 문제점

• **검색의 어려움**
파일명이나 폴더 구조에 의존한 검색만 가능하여, "이전 유사 프로젝트에서 사용한 설계 초기값"이나 "특정 설계 기준이 적용된 사례"를 찾기가 매우 어려움

• **데이터 연계의 불가능**
각 파일이 독립적으로 존재하여, "이 도면과 연결된 구조계산서는 무엇인가?", "이 보고서의 수정 이력은 어떻게 되는가?" 같은 연관 정보를 파악하기 어려움

• **이력 추적의 한계**
파일의 버전 관리가 "최종.hwp", "최종_최종.hwp", "진짜최종.hwp" 같은 수동 방식으로 이루어져, 누가 언제 왜 수정했는지 추적이 거의 불가능함

② 건설 실무자들의 AI 활용 데이터

• 단순히 최종 성과품을 정리하는 수준을 넘어서, 설계 전 과정을 AI 학습이 가능한 형태로 변환하는 '체계적인 데이터화 전략'이 필요하다.

- AI는 '무엇을 만들었는가'뿐만 아니라 '왜, 어떻게 만들었는가'까지 학습할 수 있어야 하며, 이를 위해 설계 과정의 의사결정과 변경 이력까지 체계적으로 기록하고 관리해야 한다.
- (참고) 설계 실무자들의 공통적 의견 (인터뷰 내용)
"도면, 구조계산서, 수량산출서가 AI 도입을 위해 가장 중요한 데이터"
"성과품 외에, 수정 및 협의 과정까지 이력을 추적할 수 있도록 데이터화할 필요"

5.2 AI를 위한 데이터화 전략

① 1단계 : 클라우드/온프레미스 기반 '통합 문서 플랫폼' 구축

- 전통적인 폴더 구조를 넘어서는 체계적인 문서 관리 시스템을 구축한다.
  - 기존 방식은 파일명 검색에만 의존하여 관련 문서 간 연결, 변경 이력 추적, 메타데이터 기반 검색이 불가능하기 때문에 이를 극복하기 위해 문서의 내용, 관계, 이력까지 체계적으로 관리하는 통합 플랫폼을 구축한다.

표 23 통합 문서 플랫폼의 핵심기능

- **통합 관리**
  프로젝트별 문서, 도면, 보고서, 계산서를 한 곳에서 일괄 관리
- **접근 권한 관리**
  직급, 부서, 프로젝트 참여 여부에 따라 접근 권한을 세밀하게 통제
- **버전 관리**
  문서의 모든 수정 이력을 자동으로 기록하고 추적
- **메타데이터 관리**
  프로젝트명, 작성자, 날짜, 분야, 키워드 등을 체계적으로 관리

② 2단계 : 성과품 및 내부 문서의 벡터화(Vectorization)

- AI가 문서를 이해하고 검색할 수 있도록 '벡터화' 과정을 구축한다.

※ 벡터화: 사람이 읽는 텍스트를 컴퓨터가 의미를 이해할 수 있는 숫자의 집합(벡터)으로 변환하는 과정 (예를 들어 "교량 설계"라는 단어는 [0.23, -0.45, 0.67, ...] 같은 수백 개의 숫자로 표현되고, 의미가 유사한 단어들은 유사한 벡터 값을 가지므로, 컴퓨터가 의미적 유사성을 계산할 수 있게 됨)

표 24 벡터화 파이프라인 구축 예시

- **1단계 : 텍스트 추출**
  - PDF, 한글(HWP), 워드(DOCX) 파일에서 텍스트를 추출
  - 스캔 PDF의 경우 OCR(광학 문자 인식) 처리 필수
  - 표와 이미지의 캡션도 함께 추출
- **2단계 : Chunking(의미 단위 분할)**
  - 긴 문서를 의미 있는 작은 단위로 나눔
  - 설계 문서의 경우: "한 조항", "한 테이블", "한 계산 절차" 단위로 분할
  - 너무 크면 검색 정확도가 떨어지고, 너무 작으면 맥락이 손실됨
  - 일반적으로 200~500 단어(한국어 기준 약 500~1,000자) 단위가 적절

- **3단계 : 임베딩(벡터 변환)**
  - 분할된 각 텍스트 조각을 임베딩 모델을 사용해 벡터로 변환
  - 한국어에 특화된 임베딩 모델 사용 권장 (예: Korean Sentence BERT)
  - 건설/설계 전문 용어가 포함된 모델이면 더욱 좋음
- **4단계 : 벡터DB 저장**
  - 생성된 벡터를 벡터 데이터베이스에 저장
  - 원본 텍스트, 출처 정보(파일명, 페이지 번호), 메타데이터도 함께 저장

③ 3단계 : 성과품 '결과'뿐 아니라 '과정'까지 이력 관리

- 최종 성과품뿐만 아니라 작성 과정 데이터(발주처 질의, 내부 검토 의견, 설계 변경 사유 등)까지 확보한다.
- 이를 위해 사내 그룹웨어, CDE 등 협업 플랫폼을 활용하여 각 문서의 고유 ID를 기준으로 관련 코멘트와 수정 이력이 자동 태깅되도록 구축한다.

④ 4단계 : RAG 기반 설계 기준·사내 지식 검색기 구축

- 다음의 과정으로 구성된 RAG 기반 지식 검색 파이프라인을 구축한다.
  ① 벡터DB 서버 구축 및 벡터 데이터 적재
  ② 사용자 질문을 동일한 임베딩 모델로 벡터 변환
  ③ 코사인 유사도 계산으로 상위 3~5개 관련 문서 검색
  ④ 검색된 문서를 프롬프트에 포함하여 LLM(GPT-4, Claude 등)에 전달
  ⑤ LLM이 검색 결과를 참고하여 답변 생성
  ⑥ 답변과 함께 출처 정보(문서명, 페이지, 조항)를 표시

  ※ RAG(Retrieval-Augmented Generation)란? : "검색-증강-생성"으로 번역되며, AI가 답변을 생성하기 전에 먼저 관련 문서를 검색하여 참고하는 기술이고, AI가 잘못된 정보를 만들어내는 '환각(Hallucination)' 현상을 크게 줄여줌

5.3 AI 분석에 적합한 데이터 형식

① 데이터 형식을 고려해야 하는 이유?

- AI 도입을 위한 데이터베이스(DB)를 구축할 때는 문서의 구조적 이해도, 검색 정확도, 전처리 난이도, 유지관리 비용 등 AI 성능 전반을 좌우하는 핵심 요소가 데이터 형식에 따라 크게 달라지며, 특히 실무 문서의 대표 형식인 **PDF**와 AI 친화적 형식인 **Markdown**은 각각 처리 방식과 효율성이 전혀 다르기 때문에, 어떤 형식을 선택하고 어떻게 병행할 것인지가 AI 활용 효과와 품질을 결정짓는 필수 고려사항이 된다.

② Markdown 형식

- 장점
  - 텍스트 기반이어서 AI 벡터화와 의미 단위 청킹이 정확하게 이루어져 RAG 검색 성능이 매우 높아지고, 문서 구조를 명확하게 표현할 수 있어 규정·기준·지침과 같은 반복 조회 문서 관리에 최적이다.
  - Git 기반 버전 관리가 가능하여 문서 변경 이력 추적이 쉽고 협업 효율이 높으며, 자동 변환을 통해 PDF·HTML 등 다양한 출력물로 확장하기 용이하다.
  - 불필요한 레이아웃 정보가 없기 때문에 문서 정제 비용이 낮고, 데이터베이스 업데이트와 유지보수가 가장 경제적이다.
- 단점
  - 실무자가 Markdown 문법을 익혀야 하므로 초기 사용 장벽이 존재하고, 표·수식·도면 등 복잡한 문서를 시각적으로 완전하게 표현하기 어렵기 때문에 최종 성과품 저장용으로는 적합하지 않다.
  - 이미지·도면을 별도 파일로 관리해야 해 문서 단위 보존에는 불리하고, 발주처 제출 문서 형태로 활용할 수 없어 내부 전용 포맷으로만 사용해야 한다.

표 25 Markdown 형식

- **정의**

  문서를 간단한 문자 기호로 구조화하여 작성하는 경량 마크업 언어로, 복잡한 코딩 없이 문서를 구조화하고 HTML, PDF 등으로 변환할 수 있음

- **예시**

  “#, ##, ###” : 제목 구조를 쉽게 표현
  “**텍스트**” : 굵은 글씨
  “-” : 목록 표현
  “1.항목” : 항목 표현
  “|열|” : 표 표현



③ PDF 형식

- 장점
  - 레이아웃, 표, 이미지, 도형 등 문서의 원본 형태를 정확히 보존할 수 있어 설계 성과품·협의 문서·보고서 등 공식 문서로서의 신뢰성과 법적 효력을 확보할 수 있다.
  - 모든 장비·OS에서 동일하게 열리고 사용자가 익숙해 실무 적용성이 높으며, 발주처 제출·심의·검토 단계에서 필수적으로 요구되는 표준 문서 형식이다.

- 단점
  - 구조화된 데이터가 아니라 AI가 문단·표·항목을 올바르게 인식하기 어려워 텍스트 추출 과정에서 오류가 발생하며, 특히 스캔 PDF는 OCR 비용과 정제 부담이 크다.
  - 의미 단위로 분할하기 어려워 RAG 정확도가 Markdown 대비 크게 떨어지고, 문서 변경 이력 관리가 불가능해 DB 업데이트 효율이 낮으며 협업도 비효율적이다.

5.4 PDF와 Markdown 형식의 최적 조합 전략

① '공식 문서 저장용'은 PDF, 'AI 학습·검색용'은 Markdown으로 이원화

- 설계사는 발주처 제출·심의·협의·성과품 관리 때문에 PDF를 완전히 배제할 수 없으나, RAG 기반 AI 활용에서는 Markdown이 압도적으로 효율적이므로 원본(Official)과 AI용(Operational DB)을 분리 저장하는 것이 가장 합리적이다.

② PDF → Markdown 변환 파이프라인 구축

- 설계 기준·시방서·협의 공문 등 반복 참조 문서의 핵심 내용만 Markdown으로 변환해 AI DB에 저장하고, 원본 PDF는 별도 보존하는 "이중 저장 구조"를 운영하면 검색 정확도와 실무 재사용성을 동시에 확보할 수 있다.
- 변환·생성된 문서를 대외적으로 활용하는 경우, PDF 메타데이터(작성자 필드 등) 또는 문서 머리말에 AI 활용 사실을 함께 기록하여 투명성 확보 의무를 함께 충족하도록 한다.

③ 설계 문서 특성(표·도면·계산서)에 맞춘 하이브리드 구조

- 표·수식·도면·계산서와 같이 시각 정보가 중요한 부분은 PDF로 보존하고, 텍스트 정보(설계 기준, 설명 문구, 정의, 절차)는 Markdown으로 구조화하여 AI가 쉽게 이해하고 검색하도록 분리 관리한다.

④ RAG 기반 설계지원 시스템 구축 시 Markdown을 중심 형식으로 채택

- AI가 정확한 근거 기반 답변을 제공하려면 텍스트 구조(Heading, List, Codeblock)가 필요하므로 설계 기준·법규·내부 매뉴얼을 Markdown 중심으로 재편하면, 설계 검토·품질 검토·규정 체크 자동화의 정확성이 크게 향상된다.

6 제언

6.1 설계사 규모별 맞춤 전략의 필요성

- 설계사는 인력·예산·IT 조직의 유무에 큰 편차가 있어, 대형사와 중소사가 동일한 AI 도입 모델·인프라를 적용하는 것은 비현실적이다. LLM의 파라미터 크기에 따라 요구되는 GPU·클라우드 비용, 운영 난이도가 급격히 달라지기 때문에, 소규모 회사는 경량 모델·클라우드 기반, 대형사는 sLLM·자체 인프라 등 "규모에 맞는 선택"이 필요하다. 또한 모든 규모의 설계사에게 공통으로 중요한 것은, RAG 우선 전략·양질의 Chunking·Instruction-Tuning 등 핵심 기술 요소를 이해하고, 자신의 여건에서 감당 가능한 수준으로 단계적으로 적용하는 현실적인 로드맵을 수립하는 것이다. 설계사는 인원 수, 예산 규모, IT 조직의 유무, 기술 역량에 따라 AI 도입 방식이 크게 달라질 수밖에 없으므로, 100명 규모의 중소 설계사에 500명 규모 대형사의 전략을 그대로 적용하면 실패할 확률이 높고, 반대로 대형사가 중소사의 경량 전략만 사용하면 충분한 효과를 얻지 못한다.

6.2 중소 설계사 전략

- 중소 설계사는 범용 AI와 간단한 RAG 문서 검색기부터 도입해 초기 비용을 최소화하는 것이 현실적이다. 우선 프로젝트 폴더 구조와 파일명 규칙을 정비하고, 신입·초급 엔지니어 1~2명을 지정해 성과품·기준서 PDF를 정리·정제하는 역할을 맡기는 것이 좋다. 이렇게 모은 문서를 기반으로 "설계 기준·내부 지침 RAG PoC"를 먼저 만들어 사용해 보면서, 실제로 편해진 업무를 중심으로 점진적으로 범위를 넓히는 전략이 효과적이다.

6.3 중대형 설계사 전략

- 중대형 설계사는 부서 파견형 AI TF를 운영하여 각 본부·부서의 요구를 반영한 적용 과제를 발굴하고, 설계 기준·성과품 중심의 벡터DB + RAG 시스템을 구축하는 것이 핵심이다. 월 1회 AI 활용 사례 공유와 연 1회 경진대회를 통해 실무자가 스스로 아이디어를 제안하고 확산시키는 문화도 함께 만들어야 한다. 도로부·교량부 등 핵심 부서를 파일럿 부서로 선정해 보고서 작성·설계검토·성능 검토 프로세스에 AI를 단계적으로 얹어보면서, 성공한 패턴을 회사 표준(SOP)으로 정착시켜 가는 방식이 효과적이다.

6.4 대형 설계사 전략

- 대형 설계사는 사내 sLLM(건설 분야 특화 학습된 소규모 언어 모델)+ RAG 통합 플랫폼을 중장기 목표로 삼고, 도면·BIM 모델 수준의 자동 품질 검토와 설계 지원 기능까지 포함한 "디지털 설계 플랫폼"을 지향하는 것이

바람직하다. 이를 위해 LLM, 인프라, 정보보안, 윤리, 기획이 모두 참여하는 전사 거버넌스를 구성하고, 공공부문 초거대 AI 도입 절차(보안 등급, 클라우드 구성, Ops 체계 등)를 참고해 사내 기준을 제도화해야 한다. 초기에는 규정·시방·과거 프로젝트 기반 RAG를 전사 포털에 올려 "사내 설계 지식 검색기"를 실질적인 공통 도구로 만들고, 이후 도면 검토·수량 검증 등 고도화 기능을 모듈식으로 붙여 가는 단계적 접근이 안전하다.

용어 정리

- **벡터 데이터베이스** : 고차원 벡터 임베딩을 저장, 관리, 검색하도록 설계된 특수 데이터베이스
- **벡터화** : 자연어를 컴퓨터가 이해할 수 있는 형태의 숫자들의 집합(벡터)으로 변환해주는 과정
- **임베딩** : 컴퓨터가 단어나 문장의 의미를 이해할 수 있도록 수학적으로 표현하는 것
- **클라우드** : 인터넷을 통해 서버, 데이터베이스, 소프트웨어 등의 컴퓨팅 자원을 빌려 쓰는 IT 환경
- **토큰** : AI가 텍스트를 이해하고 처리하기 위해 사용하는 텍스트의 기본 단위
- **프론트엔드** : 외부에 노출되는 인터페이스를 담당하여 다양한 유형의 데이터를 처리하고 내부 처리를 도맡는 백엔드 계층에 건네주는 계층
- **피드백 루프** : 어떠한 행동의 결과가 원인에 영향을 미쳐, 다음 결과를 강화하는 구조
- **환각 현상** : 대화형 인공지능이 대화를 생성할 때, 사실과는 전혀 다른 말을 마치 사실인 듯 답변하는 현상
- **API(Application Programming Interface)** : 두 소프트웨어 애플리케이션이 서로 데이터를 교환할 수 있도록 하는 규칙 또는 프로토콜
- **AX(AI Experience)** : 인간이 AI 도구와 상호작용하는 과정에서 경험하는 감성적 몰입, 통제감, 창의성 인식, 효율성, 결과 만족도 등 전반적인 사용자 경험을 포괄하는 개념
- **Chunking** : 문장의 단어들을 각각으로 구별하지 않고, 같은 의미를 한 덩어리로 인지하는 것
- **DX(Digital Transformation)** : 디지털 전환
- **Fine-tuning** : 모델이 기존에 학습한 지식을 새로운 데이터나 작업에 맞게 미세 조정하는 과정
- **Instruction-Tuning** : 대규모 언어 모델을 사용자가 제공하는 지시문에 더 잘 따라서 응답하도록 미세 조정하는 과정
- **KPI(Key Performance Indicator)** : 핵심 성과 지표
- **LLM(Large Language Model)** : 대규모 언어 모델
- **OCR(Optical Character Recognition)** : 이미지 속 문자를 컴퓨터가 읽을 수 있는 텍스트 데이터로 변환하는 기술
- **PEFT(Parameter-Efficient Fine-Tuning)** : 일부의 파라미터 조정만으로 특정 작업에 적합하도록 만드는 기법
- **PoC(Proof of Concept)** : 기존 시장에 없었던 신기술이나 개념을 도입하기 전 이를 검증하기 위한 과정
- **RAG(Retrieval-Augmented Generation)** : 검색증강생성, 대규모 언어 모델이 답변을 생성하기 전에 외부 지식 베이스에서 관련 정보를 검색하여 활용하도록 하는 기술
- **vLLM** : 대규모 언어 모델이 대규모 데이터를 처리할 때 계산을 더 빠르고 효율적으로 수행할 수 있도록 지원하는 오픈소스 코드 모음

설계 엔지니어링을 위한 AI 도입 가이드라인

발 행 일 : 2026년 8월
발 행 인 : 한명식
발 행 처 : 한국엔지니어링협회

주　　소 : 서울시 동작구 남부순환로 2017
전　　화 : 02-3019-3200
팩　　스 : 02-3019-3300
홈페이지 : www.kenca.or.kr

※ 이 가이드라인은 한국엔지니어링협회 허락 없이 무단으로 복제·배포·가공할 수 없습니다.

※ 본 가이드라인의 저작권은 한국엔지니어링협회에 있으며, 내용에 관한 문의는 한국엔지니어링협회로 연락하여 주시기 바랍니다.