

# Digitalisering som muliggjør mer **effektiv håndtering** av teknisk informasjon og **oppfølging** av sikkerhetssystemer i design og drift



Mary Ann Lundteigen (NTNU) (presenterer) og Maria Vatshaug Ottermo (SINTEF)



**SINTEF**



**NTNU**

## Fra omtalen av konferansen

«Når vi skifter utstyr i anleggene våre, vil **ny teknologi og enklere integrasjon** mot eksisterende kontrollsystem kunne gi oss **muligheter i et levetidsperspektiv som vi ikke har hatt tidligere**».

Dette er viktig også for **instrumenterte sikkerhetssystemer**



# Bakgrunn for presentasjonen



Shenae Lee  
(SINTEF)



Solfrid Håbrekke  
(SINTEF)



Mary Ann Lundteigen  
(NTNU)



Maria V. Ottermo  
(SINTEF)

- **Team i SINTEF/NTNU** som jobber pålitelighet og sikkerhetsanalyser av **instrumenterte sikkerhetssystemer**
- **Utforsker bruk av digitaliseringsteknologi** for å gjøre dette på en mer effektiv og mindre ressurskrevende måte
- Relevans her: **Bedre kontroll på sikkerheten gir bedre innsikt om levetid.**

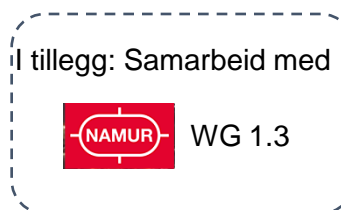


# APOS prosjektene

- APOS: Automatisert prosess for oppfølging av sikkerhetssystemer.

- **APOS (1.0):** 2019-2023
- **APOS 2.0:** 2023-2026

- Prosjektledelse: SINTEF
- Prosjekteier: Kongsberg Maritime
- Sentrale partnere med fra olje og gassindustri:



- Forankret i PDS forum (25 partnere)

## APOS Publications



### Guidelines for standardised classification and failure reporting for safety equipment in the petroleum industry

This document provides guidance on how to report and classify failure and maintenance data for safety equipment, as a basis for improved follow-up and future automation, and is a main delivery from the APOS project. Standardised equipment grouping, equipment properties and simplified failure taxonomies are suggested. For future digitalisation, the guideline also identifies standardised equipment properties and associated property values to enable establishment of a complete information model for functional safety. The suggested taxonomies and properties have therefore been compared and mapped against recognised standards and relevant electronic equipment libraries.

Read report



### Potential for automated follow-up of safety equipment

Essential means to follow up safety-critical equipment are the reporting, classification and analysis of failure data. Experience shows that considerable manual effort is needed to attain high-quality data, and therefore, this report investigates possibilities for automated failure reporting and failure class determination.

Read report



### Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase:

This guideline describes a best practice for follow-up of safety instrumented systems (SIS) during operation of a process facility. It covers management of functional safety, operation, maintenance, monitoring, and management of change. Methods for updating failure rates and optimising test intervals are presented. The document is an update of SINTEFs SIS follow-up guideline published in 2008 and 2021.

Read report



### Information model for functional safety

The information model for functional safety is based on a complete model of the distribution of the

<https://pds-forum.com/apos-publications>  
<https://pds-forum.com/apos-2-0-publications>



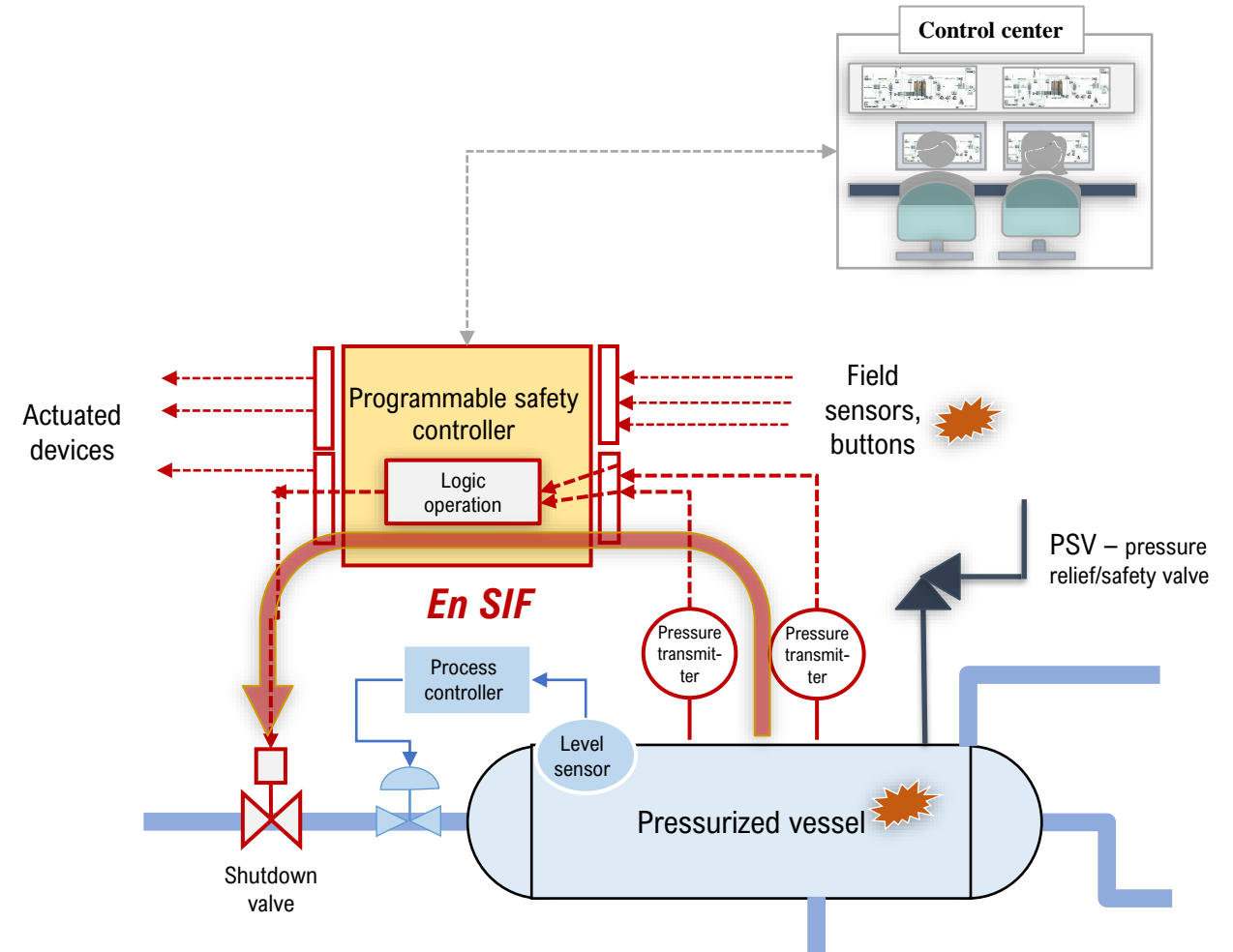
# Hva er et instrumentert sikkerhetssystem (SIS)?

Systemer **dedikert** (og uavhengig) til å **håndtere farlige hendelser**:

- Prosessnedstenging (PSD)
- Nødavstengning (ESD)
- Brann og gass deteksjon (F&G)
- Instrumentert sekundær overtrykksbeskyttelse («HIPPS»)

Hva **skiller** disse systemene fra andre:

- Spesifikke regelverkskrav
- Detaljerte livssyklus krav i standarder og retningslinjer (IEC 61508/IEC 61511)
- Pålitelighetskrav (SIL krav) til enkelt-funksjoner (SIFer) forankret i risikoanalyser
- Krav til oppfølging av pålitelighetskrav av SIFer i driftsfasen



# Den viktige koblingen mellom design og drift

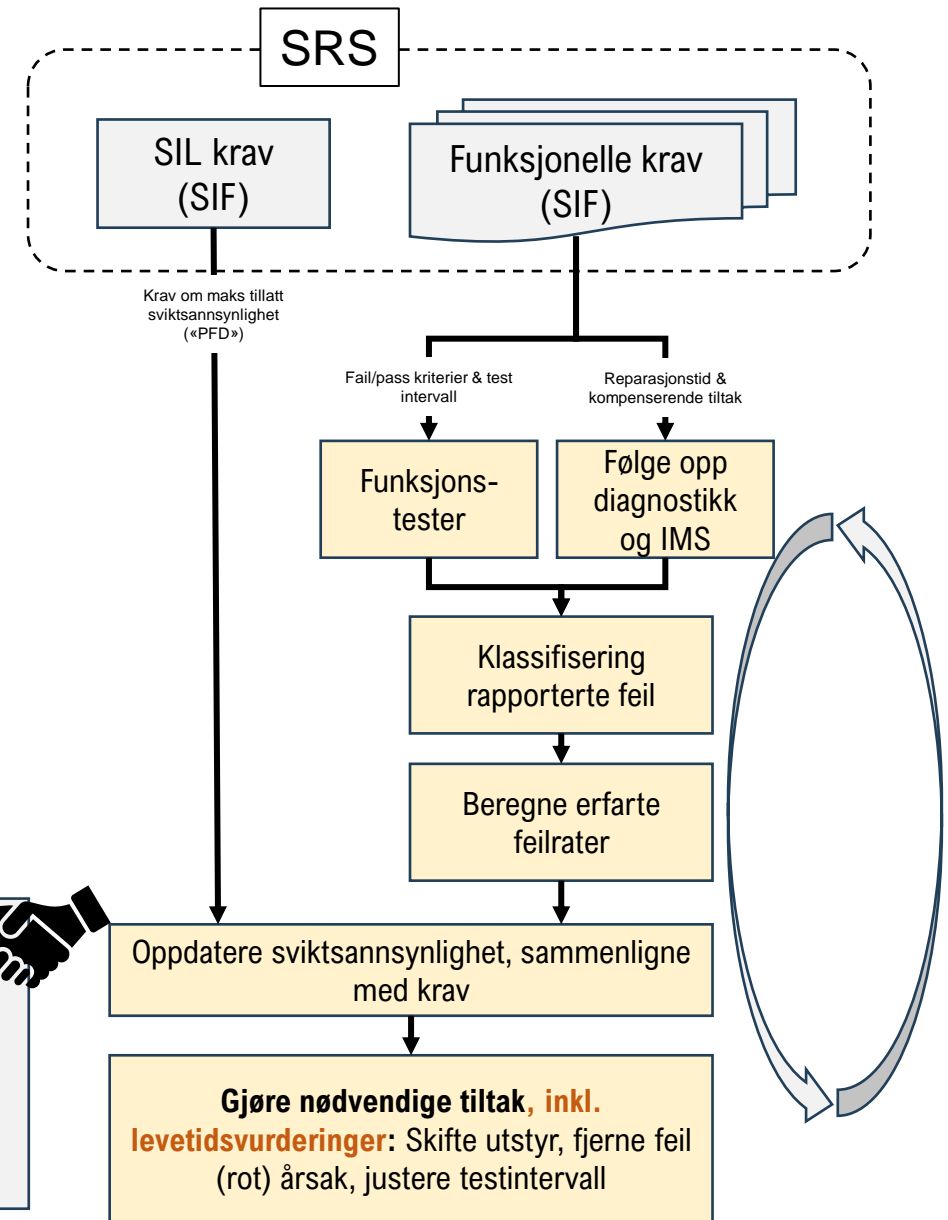
## Utvikle kravdokument (SRS)

IEC 61511 req. #	Requirement description
a	SIF description
b	A list of the plant input and output devices related to each SIF
c	Requirements to identify and take account of common cause failures
d	A definition of the safe state of the process for each identified SIF
e	A definition of any individually safe process states
f	The assumed sources of demand and demand rate on each SIF
g	Requirements relating to proof test intervals
h	Requirements relating to proof test implementation
i	Response time requirements for each SIF
j	The required SIL, mode of operation and PFD (or PFH) if relevant
k	SIS process measurements, range, accuracy, and their trip points
l	A description of SIF process output actions
m	The functional relationship between process inputs and outputs
n	Requirements for manual shutdown for each SIF
o	Requirements relating to energize or de-energize to trip for each SIF
p	Requirements for resetting each SIF after a shutdown
q	Maximum allowable spurious trip rate for each SIF
r	Failure modes for each SIF and desired response of the SIS
s	Procedures for starting up and restarting the SIS
t	All interfaces between the SIS and any other system
u	Modes of operation of the plant and associated SIF requirements
v	The application program safety requirements
w	Requirements for bypasses including written procedures to be applied
x	Any [manual] action necessary to achieve or maintain a safe state
y	The mean repair time which is feasible for the SIS
z	Dangerous combinations of output states of the SIS
aa	Identification of the extremes of all environment conditions

## Samle inn driftsrelaterte data:

- Rapporterte feil (utstyr og per utstyrsgupper)
- Feilmoder
- Valgte testintervall
- Feilårsaker
- «Demands» (reelle aktiveringer)

«Kontroll med levetid handler om å ha kontroll på både krav og historikk»



... og vise at valgte løsninger er gode nok!



**SIL:** Safety integrity level

**IMS:** Information management system (fra kontrollsystem)

# Erfarte utfordringer

## Krav og designdokumentasjon



Format (pdf, word, excel) lite egnet for automatisk og sømløs utveksling

Samme data må (delvis) manuelt til andre systemer (i flere runder)

## Digitale plattformer for håndtering og analyse av data

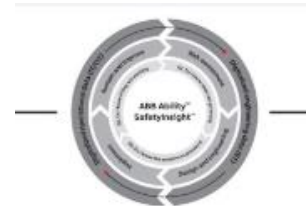
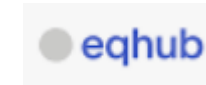


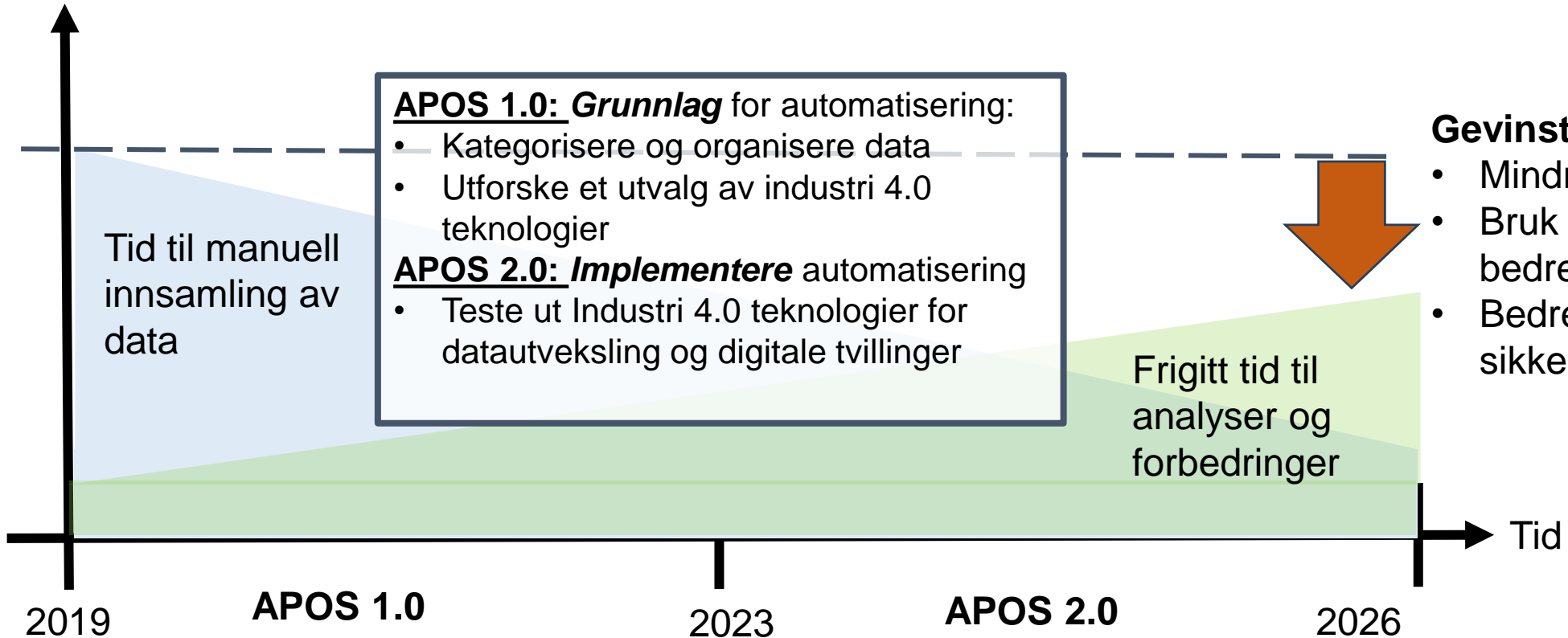
ABB Ability™ SafetyInsight™  
DCS agnostic suite of applications



Mange **gode software applikasjoner** for håndtere data og utføre analyse, men å få **data inn og utveksle** mellom systemer krever **manuell innsats og spesialløsninger**.

# APOS prosjektenes fokus på digitalisering

Ressursbruk



**Gevinst:**

- Mindre ressursbruk
- Bruk av ressurser på bedre måte
- Bedre kontroll med sikkerhet





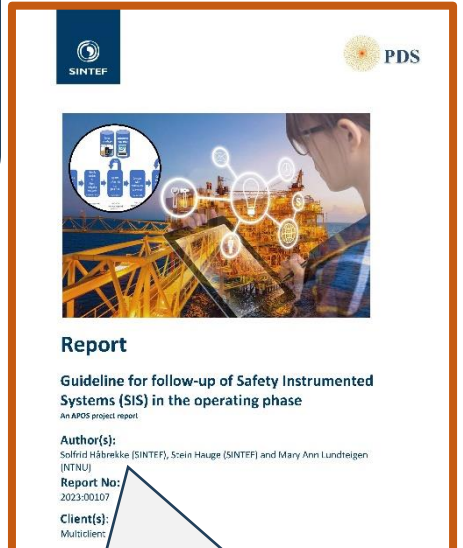
# APOS 1.0 Bygge grunnmuren og utforske teknologier for sømløs integrasjon



Testet ut **automatisk feil-klassifisering**:

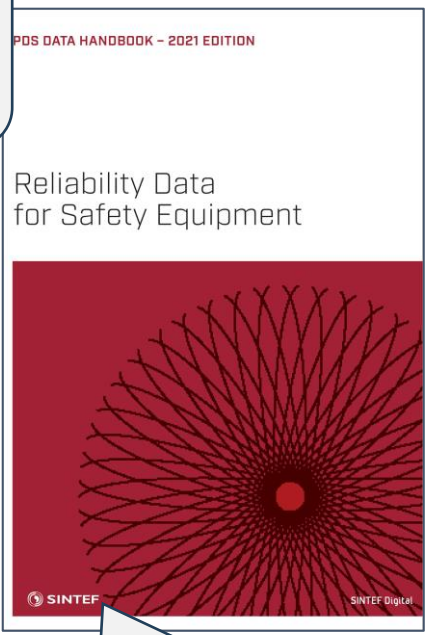
- Regelbasert – fra SAP koder
- KI-basert («TLP») – tolke fritekst

- Identifiserte **pålitelighets-påvirkende faktorer** per utstyrstype
- Koblet egenskaper om utstyr definert i IEC standard 61897 og tilhørende koder i IEC CDD



- En oppdatering av en tidligere retningslinje – **praktiske metoder for å følge opp SIL krav.**
- **For bruk til pålitelighetsoppfølging av SIF i drift**

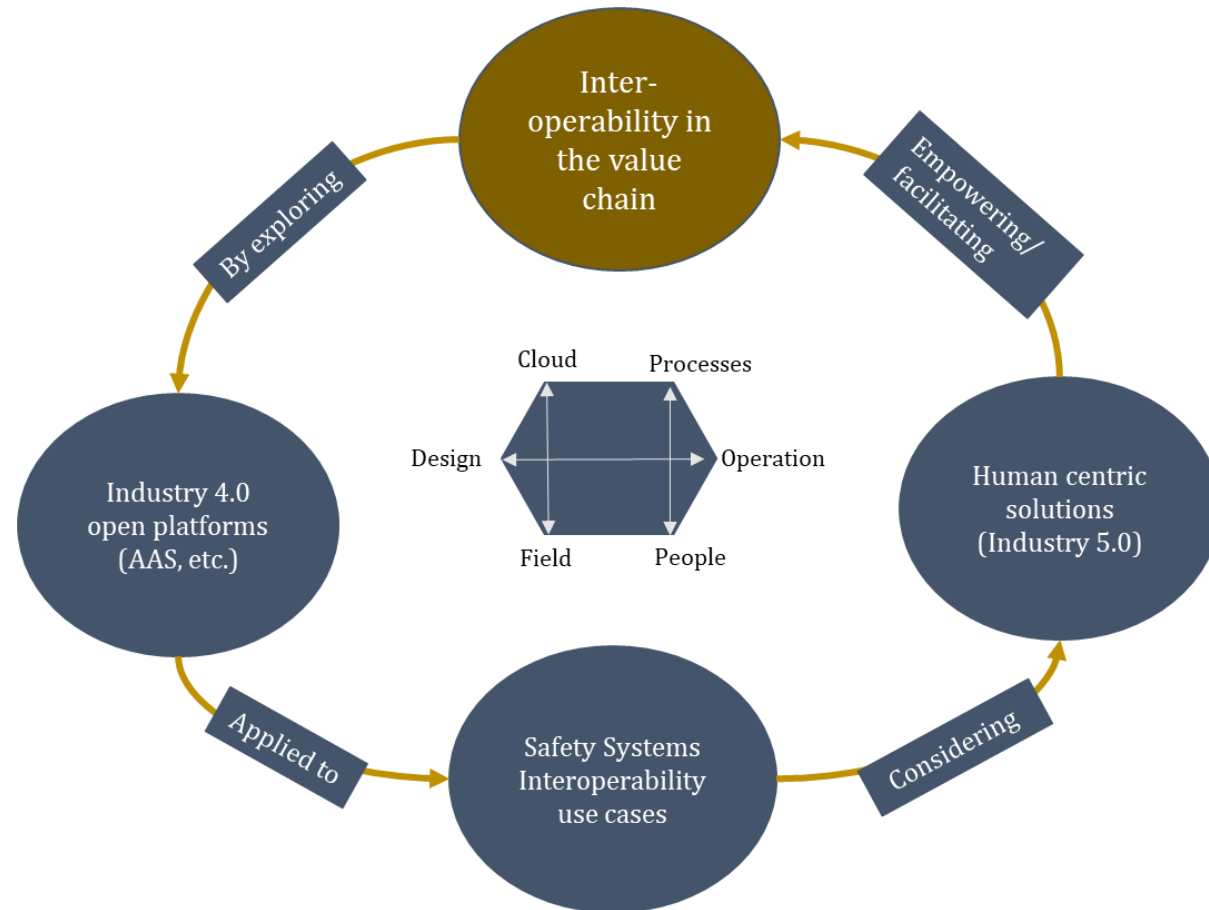
- Første forslag til en **informasjonsmodell** basert på SRS krav, SIS utstyr og SIFer (votering,..)



- Oppdatering av **generiske feildata** for bruk i prosjekter – basert på analyse av et **stort nytt og utvidet datasett** om feil erfart i drift



# APOS 2.0: Ta i bruk (et utvalg av) teknologier for å oppnå interoperabilitet



Oversikt over APOS 2.0 hovedaktiviteter



# APOS 2.0: Ta i bruk (et utvalg av) teknologier for **interoperabilitet**

**Bred samstemthet om betydning**  
(eks: Definert i en internasjonal standard)

**Maskinlesbart – med unik kode og kodeformat**

**SHARED** and **FORMAL**

**Interoperabilitet** – *Evne* til å kunne utveksles mellom maskiner (software applikasjoner)

**Bryter #1234**

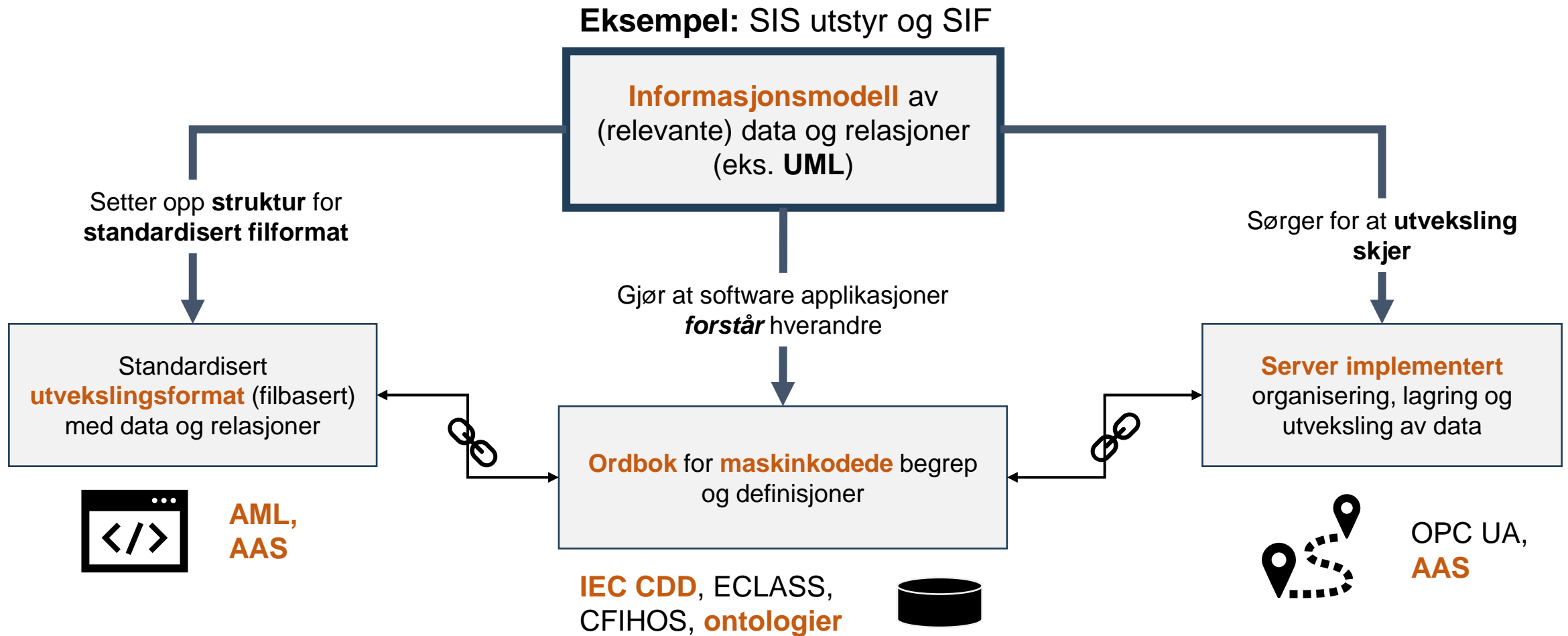


**Bryter #8999**

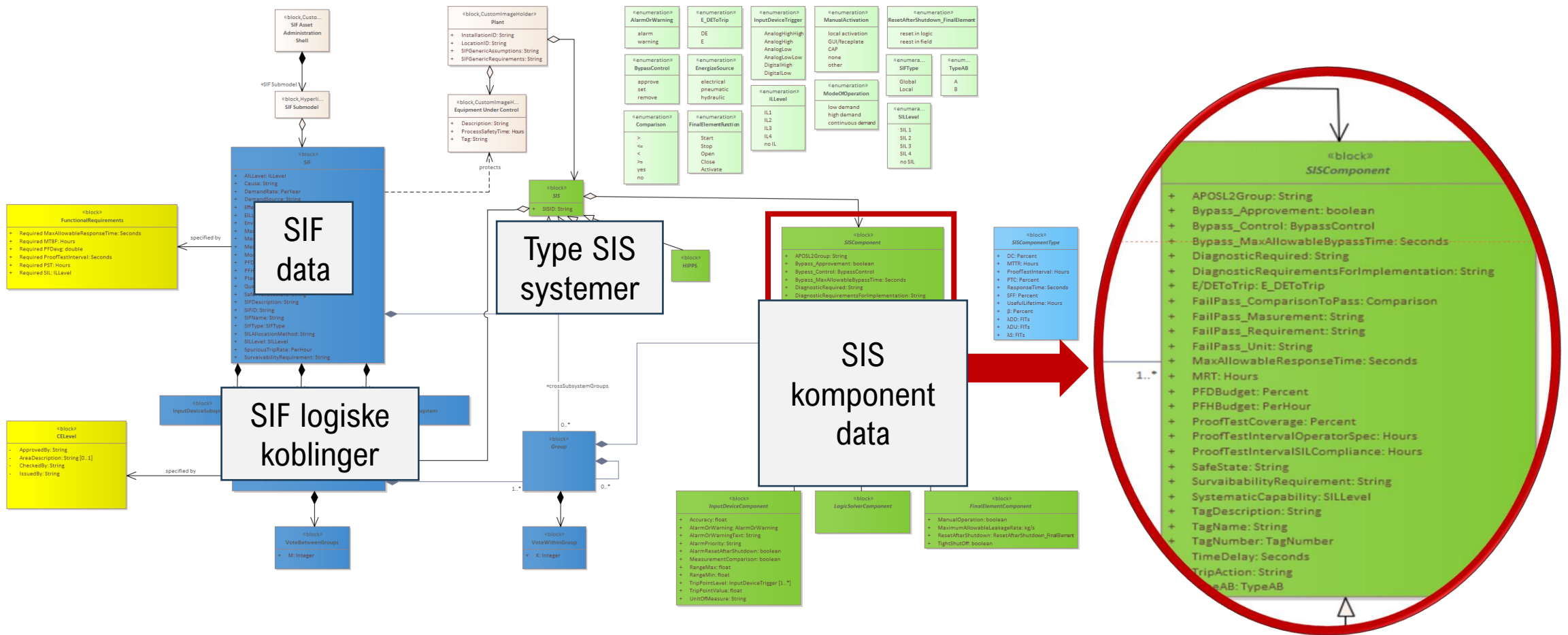


# Eksempler på byggeklosser for interoperabilitet

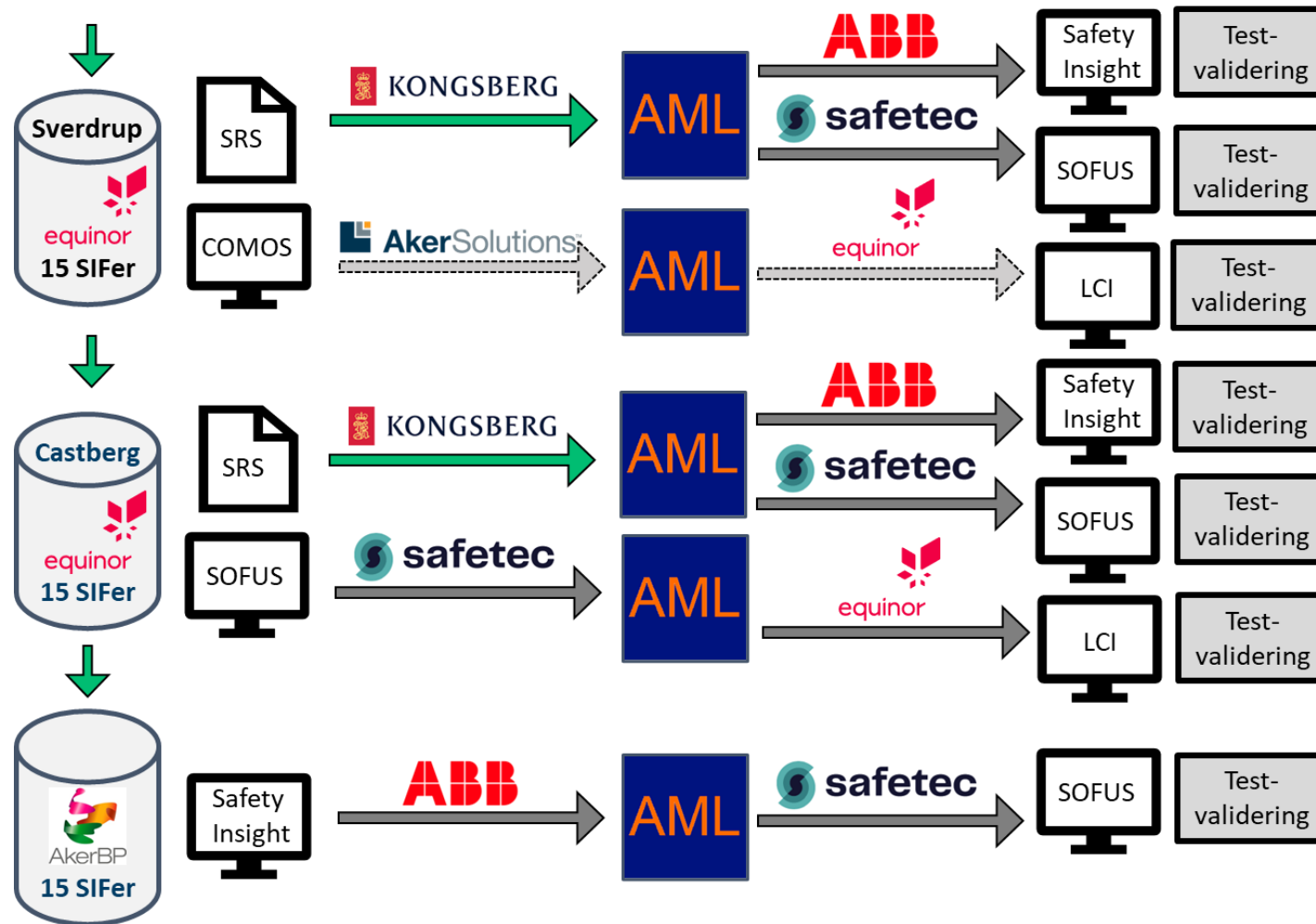
**UML:** Unified modeling language  
**AML:** Automation Mark-up language  
**AAS:** Asset administration shell  
**CDD:** Common data dictionary  
**CFIHOS:** Capital Facilities Information Hand Over Specification  
**ECLASS:** Electronic Classification and Standardization  
**OPC UA:** Open Platform Communications Unified Architecture



# APOS 2.0: Bygget UML modell for data relatert til SIF og SIF komponenter



# APOS 2.0 piloter: Eksportert UML modell til AML som utvekslingsformat

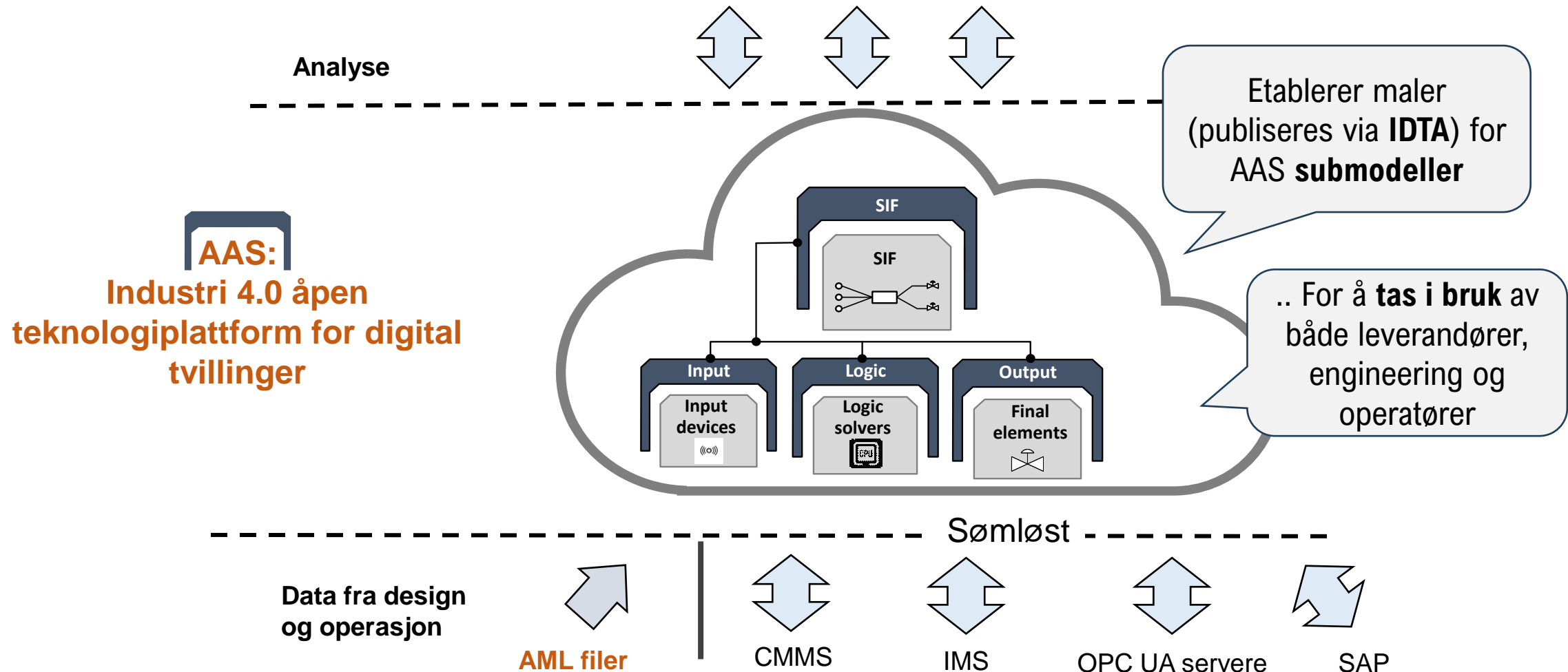


AML: Automation Markup Language («XML format»)



# APOS 2.0: Bygger struktur for **digital tvilling** for SIS/SIF med **AAS**

Applikasjoner for overvåkning og analyse – *inkludert levetidsanalyser*



# APOS 2.0: Leder arbeid med AAS submodeller for SIF/SIF i regi av IDTA

Home > Content Hub > Submodels

## AAS Submodel Templates

Submodels constitute the content of the Asset Administration Shell. They describe content-related or functional aspects of an asset. Find the overview of the official IDTA submodel templates here.

IDTA SUBMODELS

### Registered AAS Submodel Templates

You would like to develop your own submodel templates or collaborate in the development of the listed submodel templates? Find the process described [here](#). For further questions, contact us via [email](#).

Number of our submodels: **93**

Arbeidsgruppe med norske og internasjonale medlemmer fra leverandører og brukere (operatører)

Startet opp August 2024. Planlagt avsluttet sommeren 2025. Har møter online hver 14 dag.

Submodel Template	IDTA Number ⓘ	Version	Status	Downloads & Links
Safety instrumented functions (SIF) for the process industries	02064	1.0	In Development	Coming soon



# APOS 2.0: Leder arbeid med å utvide IEC CDD med SIF/SIF begrep, definisjoner og maskinlesbare koder

The screenshot displays the IEC Common Data Dictionary (CDD) web interface. The header shows the IEC logo and the title 'International Electrotechnical Commission IEC 61987 - IEC/SC 65E - Common Data Dictionary (CDD - V2.0018.0002)'. A search bar contains the text 'safe state' and is followed by an 'OK' button. Below the search bar, there are radio buttons for filtering results: 'Classes', 'Properties', 'Value lists', 'Value terms', 'Units', 'Lists of Units', 'Relations', 'DET classification', and 'All kind of items' (which is selected). A 'hit' section shows 'Property 0112/2///61511#SLO Safe state' with options to 'Export selected', 'Select all', and 'Deselect all'. The main content area is a table with a 'PROPERTY' header and a table of properties for the selected item. The table has columns for the property name and its value. The values are highlighted in yellow in the original image.

PROPERTY	
Code:	0112/2///61511#SLO
Version:	001
Revision:	01
IRD:	0112/2///61511#SLO100#003
Preferred name:	Safe state
Synonymous name:	
Symbol:	
Synonymous symbol:	
Short name:	
Definition:	state of the process when safety is achieved
Note:	
Remark:	
Primary unit:	
Alternative units:	
Level:	
Data type:	string
Format:	
Property constraint:	
Definition source:	IEC 61511
Property data element type:	DEPENDENT_P_DET
Drawing:	
Formula:	
Value list code:	0112/2///61987#ABJ755
Value list:	
DET class:	
Applicable classes:	0112/2///61987#ABC538 - Process criticality classification



# Status for maler for AAS submodeller

The screenshot displays the AASX Package Explorer V3.0 interface. On the left, there are three conceptual diagrams: 'AAS: SIF' containing 'SM: SIF', 'AAS: SIS component' containing 'SM: SIS component', and a 'Submodel' diagram. The main window shows a tree view of the package structure with the following elements:

- AAS "SIF" [https://example.com/ids/sm/9484\_7002\_1142\_0797] of [https://example.com/ids/asset/9580\_9050\_1142\_6117]
  - Asset AssetInformation https://example.com/ids/asset/9580\_9050\_1142\_6117
    - SM <T> "SIF" [https://example.com/ids/sm/4184\_9050\_1142\_3460]
  - AAS "SIS\_component" [https://example.com/ids/sm/7080\_3120\_1052\_9971] of [, NotApplicable]
    - Asset AssetInformation
      - SM <T> "SIS\_Component" [https://example.com/ids/sm/7272\_7060\_1142\_3535]
  - AAS "Equipment\_under\_control" [https://example.com/ids/sm/2065\_3180\_1142\_1083] of [, NotApplicable]
    - Asset AssetInformation
      - SM <T> "Equipment\_under\_control" [https://example.com/ids/sm/2065\_3180\_1142\_5083]
  - AAS "SIS" [https://example.com/ids/aas/5323\_7002\_1142\_2564] of [, NotApplicable]
    - Asset AssetInformation
      - SM <T> "SIS" [https://example.com/ids/sm/0233\_7002\_1142\_0213]

The right-hand pane shows the detailed view of the selected 'AssetAdministrationShell (according IEC63278)'. It includes the following metadata:

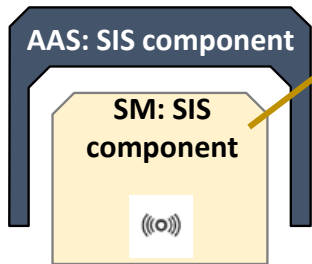
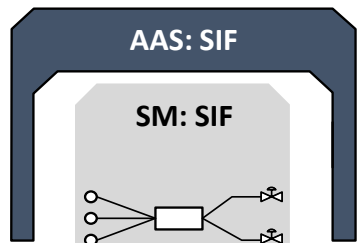
- Referable: idShort: SIF
- Identifiable: id: https://example.com/ids/sm/9484\_7002\_1142\_0797, id (Base64): aHR0cHM6Ly9leGZFcGxlLmNvbS9pZHMvc20vOTQ4NF83MDAyXzExNDhMDc5Nw==
- AssetInformation: Kind (of AssetInformation): Type, globalAssetId: https://example.com/ids/asset/9580\_9050\_1142\_6117, assetType: /SIF\_picture.PNG, specificAssetId: image/png
- DefaultThumbnail: Resource element, value: /SIF\_picture.PNG, contentType: image/png

Verktøy: AASX Package Explorer

AAS: Asset Administration Shell. SM: Submodell.



# Status for arbeid med maler for AAS submodeller



AAS Package Explorer V3.0 - local file: C:\Users\lundteig\OneDrive - NTNU\Desktop\AsoPackageExplorer\APOS\Submodel SIF data for AA study based on IEC CDD input and SRS ontology maps\_24012025.aasx buffered to: C:\Users\lundteig\AppData\Local\Temp\tmp7116

File Workspace Option Help

https://example.com/ids/sm/948  
4\_7002\_1142\_0797

**Submodel**

Submodel element

Submodel element

https://example.com/ids/asset/9  
580\_9050\_1142\_6117

- Asset "SIF" [https://example.com/ids/sm/9484\_7002\_1142\_0797] of [https://example.com/ids/asset/9580\_9050\_1142\_6117, Type]
- Asset "AssetInformation" [https://example.com/ids/asset/9580\_9050\_1142\_6117]
- SM <Tx> "SIF" [https://example.com/ids/sm/4184\_9050\_1142\_3460]
- AAS "SIS\_component" [https://example.com/ids/sm/7080\_3120\_1052\_9971] of [ , NotApplicable]
- Asset "AssetInformation" [https://example.com/ids/sm/7272\_7060\_1142\_3535]
- SM <Tx> "SIS\_Component" [https://example.com/ids/sm/7272\_7060\_1142\_3535]
- SMC "Tag\_information" (9 elements) @(Multiplicity=One)
- SMC "SRS\_requirements\_SLOP" (19 elements) @(Multiplicity=OneToMany)
- Prop "Safe\_state" @(Multiplicity=One)
- Prop "Systematic\_capability" @(enumeration=Sil 1, Sil 2, Sil 3, Sil 4) @(Multiplicity=One)
- Prop "PFD\_budget" @(Multiplicity=ZeroToOne)
- Prop "PFH\_budget" @([unit=per hour] @(Multiplicity=ZeroToOne)
- SMC "Proof\_test" (5 elements) @(Multiplicity=One)
- Prop "Maximum\_allowable\_response\_time" @([unit=seconds] @(Multiplicity=One)
- Prop "Mean\_repair\_time" @([unit=seconds] @(Multiplicity=One)
- SMC "Bypass\_requirements" (6 elements) @(Multiplicity=One)
- Prop "Energize\_or\_Deenergize\_to\_trip" @(enumeration=energized, de-energized) @(Multiplicity=One)
- Prop "Trip\_action" @(Multiplicity=One)
- Prop "Survivability\_requirement" @(Multiplicity=ZeroToMany)
- Prop "Diagnostic\_requirements\_for\_implementation" @(Multiplicity=ZeroToMany)
- Prop "Required\_diagnostic" @(Multiplicity=ZeroToMany)
- Prop "Time\_delay" @([unit=seconds] @(Multiplicity=ZeroToMany)
- SMC "Failure\_mode\_and\_its\_responses" (4 elements) @(Multiplicity=ZeroToMany)
- SMC "Input\_device\_specific" (4 elements) @(Multiplicity=ZeroToOne)
- SMC "Logic\_solver\_specific" @(Multiplicity=ZeroToOne)
- SMC "Final\_element\_specific" (4 elements) @(Multiplicity=ZeroToOne)
- Ref "SIF\_ID" @(Multiplicity=One)
- SMC "Model\_specifications" (13 elements) @(Multiplicity=One)
- SMC "Reliability\_data\_type" (11 elements) @(Multiplicity=One)
- Prop "MTBF" @([unit=years] @(Multiplicity=ZeroToOne)
- Prop "lambdaDU" @([unit=per hour] @(Multiplicity=One)
- Prop "PFD" @(Multiplicity=ZeroToOne)
- Prop "PFH" @([unit=per hour] @(Multiplicity=ZeroToOne)
- Prop "lambdaDD" @([unit=per hour] @(Multiplicity=ZeroToOne)
- Prop "lambdaSU" @([unit=per hour] @(Multiplicity=ZeroToOne)
- Prop "lambdaSD" @([unit=per hour] @(Multiplicity=ZeroToOne)
- Prop "Beta" @([unit=percentage] @(Multiplicity=One)
- Prop "SFF" @([unit=percentage] @(Multiplicity=One)
- Prop "DC" @([unit=percentage] @(Multiplicity=One)
- Prop "Data\_source" @(Multiplicity=One)
- SMC "APOS\_reliability\_influencing\_properties\_DLOP\_and\_OLOP" (7 elements) @(Multiplicity=ZeroToOne)
- Prop "Application" @(enumeration=ESD, PSD, ESD/PSD, F&G, HVAC, EDP, BPCS, HIPPS, PPS, Equipment protection, Offloading, Monitoring, Combined) @(Multiplicity=ZeroToMany)
- Prop "External\_exposure" @(enumeration=severe, moderate, shielded, indoor, outdoor) @(Multiplicity=ZeroToOne)
- Prop "Fluid\_severity" @(enumeration=clean, medium, dirty) @(Multiplicity=ZeroToOne)

Element Content

**Submodel Element (Property)**

Referable: Energize\_or\_Deenergize\_to\_trip

HasExtension:

Semantic ID:

Supplemental Semantic IDs:

Qualifiable:

Qualifier 1

kind: ValueQualifier

type: enumeration

valueType: xs:string

value: energized, de-energized

Qualifier 2

semanticId: (GlobalReference) https://admin-shell.io/SubmodelTemplates/Cardinality/1/0

kind: TemplateQualifier

type: Multiplicity

valueType: xs:string

value: One

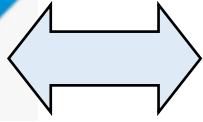
**HasDataSpecification (Reference):**

Property

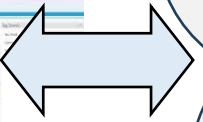
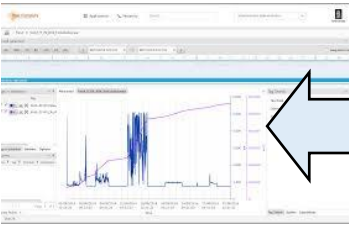
valueType: xs:string

# Målet med submodeller (i drift)

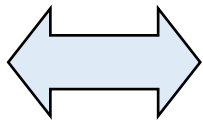
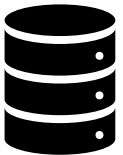
Maintenance system



IMS

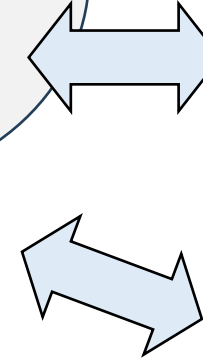


OPC UA servers



The screenshot displays a software interface for managing submodels. On the left, there are three panels: 'Submodel' with URL 'https://example.com/ids/sv/948 4\_7002\_1142\_0797', 'Submodel element', and another 'Submodel element' with URL 'https://example.com/ids/asset/9 580\_9050\_1142\_6117'. Below these is a flow diagram with 'Input element submodel', 'Logic element submodel', and 'Final element submodel'. On the right, there is a list of parameters and their types, such as 'AAS\_ID', 'AssetInformation', 'Systemic\_capability', etc.

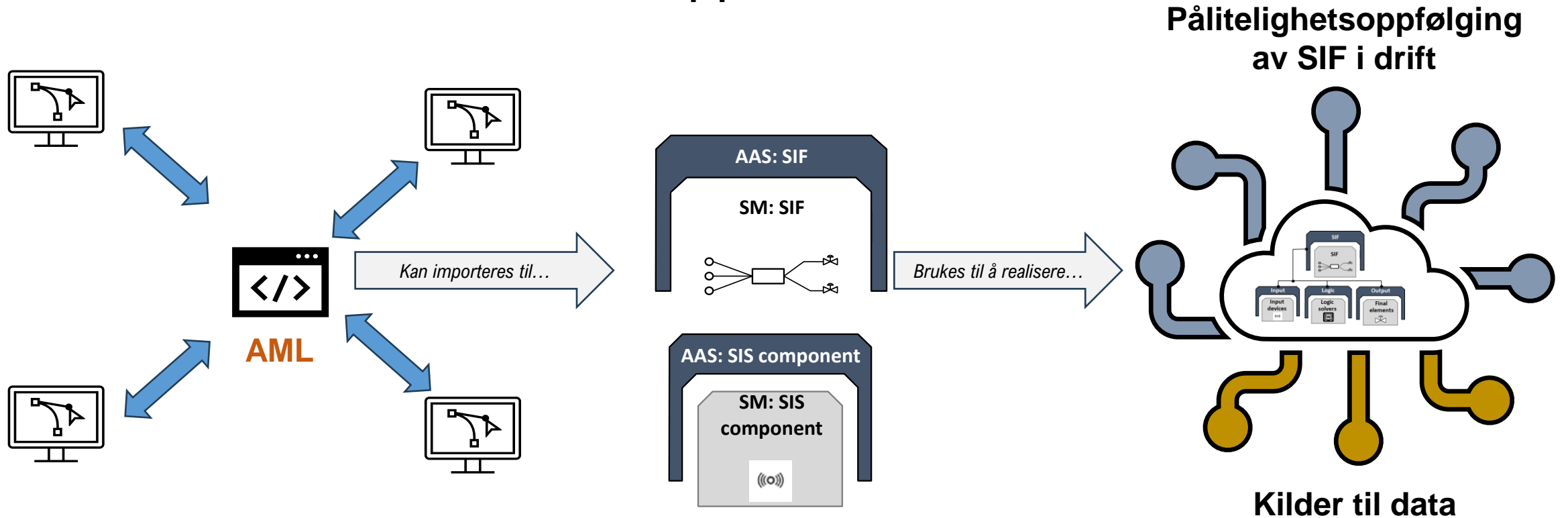
Submodellene er **maler** som tas i bruk, **tilføres data** (i design) og **overføres** til et **AAS servermiljø** for tilføring av **mer data, oppdateringer og utveksling**



IMS: Information Management System (from SAS providers). DU: Dangerous Undetected. PFD: Probability of Failure on Demand



# APOS 2.0: Hva ønsker vi å oppnå med alt dette?



Maskinlesbart og standardisert **filformat** som muliggjør **automatisk** utveksling av krav og design data mellom ulike systemer

Innføre maskinlesbare maler for **implementering av digitale tvillinger** – først i design og deretter for drift

Bidra til at industrien **tar i bruk** digitale tvillinger som «host» for data brukt til ulike typer analyser



# Utfordringer og lærepointer

- Grunnarbeid viktig – Enes om **hvilke data** er sentrale
  - Standardisering må **ikke bli særnorsk**, men koblet med internasjonale initiativ (IEC CDD, IDTA)
  - Viktig med **praktiske piloter** å teste ut – involvere kompetanse og applikasjoner hos partnerne
- 
- Mye datateknikk – (for mange av oss) = nye begrep og teknologier ...
  - Forstå begrensninger utfra modenhet i teknologiene
  - **Og ikke minst:** Hensynta de som skal jobbe med verktøyene



Takk for oppmerksomheten!



Svarer gjerne på spørsmål!

Følg gjerne APOS prosjektet via <https://pds-forum.com/>.  
Vi svarer også på spørsmål i etterkant.



Shenee Lee  
(SINTEF)



Solfrid Håbrekke  
(SINTEF)



Mary Ann Lundteigen  
(NTNU)



Maria V. Ottermo  
(SINTEF)