SCADA
Operator Interface
*interface homme machine*
Mensch-Maschine Kommunikation
Prof. Dr. H. Kirrmann
ABB Research Center, Baden, Switzerland
Control room

Two human interfaces: old style mimic board (behind) and screens (front)
SCADA functionality

Data acquisition and display
store binary & analog data into process data base

Alarm & Events
record important changes and operator actions

History data base
keep a record of the process values

Measurand processing
calculate derived values (limit supervision, trending)

Logging & reporting

Human Machine Interface (HMI):
graphical object state presentation, lists, reports

Operator Command handling
binary commands, set points
recipes, batches, scripts (command procedures)

Interfacing to planning & analysis functions: CMMS, …
Operator workplace: three main functions

- Current state
- Alarms and events
- Trends and history
# Human-Machine Interface to Plant (HMI-P)

| Representation of process state | • Lamps, instruments, mimic boards  
|                               | • Screen, zoom, pan, standard presentation  
|                               | • Actualization of values in the windows  
|                               | • Display trends and alarms  
|                               | • Display maintenance messages  
| Protocol of the plant state   | Recording process variables and events with time-stamp  
| Dialog with the operator      | Text entry, Confirmation and Acknowledgments  
| Forwarding commands           | Push-buttons, touch-screen or keyboard  
| Record all manipulations      | Record all commands and especially critical operation (closing switches)  
| Mark objects                  | Lock objects and commands  
| Administration                | Access rights, security levels  
| On-line help                  | Expert system, display of maintenance data and construction drawings, internet access  

### Human-Machine Interface to Engineering (HMI-E)

| Configuration of the plant | • Bind new devices  
|                           | • Assign names and addresses to devices  
|                           | • Program, download and debug devices  
| Screen and Keyboard layout | Picture elements, Picture variables, assignment of Variables to Functions  
| Defining command sequences | Command language  
| Protocol definition | What is an event and how should it be registered?  
| Parameterize front-end devices | Set points, limits, coefficients  
| Diagnostic help | Recording of faulty situations, fault location, redundancy handling  

Mainly used during engineering and commissioning phase, afterwards only for maintenance and modifications of the plant.  
Used more often in flexible manufacturing and factory automation.
Local Operator Console (printing)
Example: Siemens

Workstations

PLCs

Field devices

OTHER PLANT AREAS

LAB
PACKAGING
QUALITY
WAREHOUSE

PROCESSING

SUPERVISORY
OPERATOR
ENGINEERING

REDUNDANT SINEC H1

SINEC L2 DP

MOTOR DRIVE
PRESSURE TRANSMITTER
VISION SYSTEM
REACTOR

www.aut.sea.siemens.com/pcs
Functions of the operator interface

- Process Graphics
- Event/Alarm Manager
- Trends
- Historian
- Controller Integration
- Recipes
Trends:
disappearance of custom HMI, increasing access over Windows (Internet Explorer),
data entry by keyboard, touch screen, trackball (seldom mouse), buttons (hard-feel).
Example of Screen (EPFL air condition)
Example of Screen

Log

View
Each screen object can represent several process variables....
Alarm and Event Management

time stamps exact time of arrival (or occurrence)
categorize by priorities
log for further use
acknowledge alarms
prevent multiple, same alarms
remove alarms from screen once reason disappeared (but keeps them in the log)
link to clear text explanation
What is an alarm, an event?

A&E consider changes occurring in the plant (process) or in the control system (operator actions, configuration changes, …) that merit to be recorded.

Recorded changes can be of three kinds:
- informative: no action required
  (e.g. "production terminated at 11:09")
- warning: plant could stop or be damaged if no corrective action is taken "soon"
  (e.g. "toner low")
- blocking: the controller took action to protect the plant and further operation is prevented until the reason is cleared (e.g. "paper jam")

In general, warnings and blocking alarms should be acknowledged by the operator ("quittancer", "quittieren").

An alarm is not necessarily urgent, several levels of severity may be defined.

An event is a change related to:
  operator actions ("grid synchronisation performed at 14:35"),
  configuration changes ("new software loaded in controller 21"), and
  system errors ("no life sign from controller B3")
What triggers an alarm?

- binary changes of process variables (individual bits), some variables being dedicated to alarms

- reception of an analog variable that exceeds some threshold (upper limit, lower limit), the limits being defined in the operator workstation

- reception of an alarm message (from a PLC that can generate such messages)

- computations in the operator workstation (e.g. possible quality losses if current trend continues)

- calendar actions (e.g. unit 233 did not get preventive maintenance for the last three months)
Implementing alarms by variables

An alarm is often encoded as a simple 16-bit word sent by an object (thru PLC) in the plant. Each bit has a different meaning, the error condition is reset when the word is 0.

This coding allows to display the error message in several national languages. A database contains the translations.

Problem: keep devices and alarm tables in the operator workstation synchronized
Example of a log: states, alarms,

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3.02 13:40</td>
<td>Gpcpt2ofpbonne</td>
<td>4824</td>
</tr>
<tr>
<td>12.3.02 13:40</td>
<td>Gpt2bac</td>
<td>50</td>
</tr>
<tr>
<td>12.3.02 13:40</td>
<td>Gpcpt2bac</td>
<td>70</td>
</tr>
<tr>
<td>12.3.02 13:40</td>
<td>Gpcptbe2</td>
<td>45</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gpcpt1bac</td>
<td>151</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gpcpt1ofpbonne</td>
<td>4826</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gcptaes2</td>
<td>45</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gpt1bac</td>
<td>49</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gpt1bac</td>
<td>49</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gpdefr2</td>
<td>64</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gpvoydef</td>
<td>2</td>
</tr>
<tr>
<td>12.3.02 13:41</td>
<td>Gpr3tempscycleprd</td>
<td>318</td>
</tr>
<tr>
<td>12.3.02 13:42</td>
<td>Gpstr1e1</td>
<td>16</td>
</tr>
<tr>
<td>12.3.02 13:42</td>
<td>Gpalarme1</td>
<td>0</td>
</tr>
<tr>
<td>12.3.02 13:42</td>
<td>Gpalarme2</td>
<td>0</td>
</tr>
<tr>
<td>12.3.02 13:42</td>
<td>Gpstr1e1</td>
<td>240</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpetatmodemarche</td>
<td>2</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpts cycle</td>
<td>1346</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpetatmodemarche</td>
<td>1</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpdefge1</td>
<td>16</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpetatmodemarche</td>
<td>0</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpts cycle</td>
<td>317</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpdefr2</td>
<td>0</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpvoydef</td>
<td>0</td>
</tr>
<tr>
<td>12.3.02 13:43</td>
<td>Gpdefge1</td>
<td>0</td>
</tr>
<tr>
<td>12.3.02 13:44</td>
<td>Gpetatmodemarche</td>
<td>1</td>
</tr>
<tr>
<td>12.3.02 13:44</td>
<td>Gp2tempscycleprd</td>
<td>1992</td>
</tr>
<tr>
<td>12.3.02 13:44</td>
<td>Gpts cycle</td>
<td>435</td>
</tr>
<tr>
<td>12.3.02 13:44</td>
<td>Gpalarme3</td>
<td>1</td>
</tr>
<tr>
<td>12.3.02 13:44</td>
<td>Gpalarme4</td>
<td>1</td>
</tr>
<tr>
<td>12.3.02 13:44</td>
<td>Gpalarme3</td>
<td>0</td>
</tr>
<tr>
<td>12.3.02 13:44</td>
<td>Gpcpt2ofpbonne</td>
<td>4823</td>
</tr>
</tbody>
</table>

GP: Compteur 2 Ordre de Fabrication Pece bonne MD
Compteur pieces dans bac
GP Compteur pieces B equipe 2
GP Compteur pieces A equipe 2
Compteur pieces dans bac
MOT32_GP
GP: Mot R3 Temps de Cycle de Production
GP: [Str1E1] Affichage des informations des présences pièces (outilage 1)
GP: Mot 1 alarme
GP: Mot 2 alarme
GP: [Str1E1] Affichage des informations des présences pièces (outilage 1)
GP: Etat du mode de marche: MANUAL
GP Temps de cycle cellule
GP: Etat du mode de marche
MOT1: Arret d'urgence robot 3
GP: Etat du mode de marche
GP Temps de cycle cellule
MOT32_GP
GP: Etat du mode de marche: AUTOMATIQUE
GP: Mot R2 Temps de Cycle de Production
GP Temps de cycle cellule
GP: Mot 3 alarme
GP: Mot 4 alarme
GP: Mot 3 alarme
GP: Compteur 2 Ordre de Fabrication Pece bonne MD
## Alarm messages

As bandwidth became available, devices can send alarm and event messages instead of alarm variables.

These messages include alarm details, and especially environment information (under which circumstances did the alarm occur)

<table>
<thead>
<tr>
<th>Event</th>
<th>Format</th>
<th>Plant State</th>
<th>Event Number</th>
<th>Object</th>
<th>Environment 1</th>
<th>Environment 2</th>
<th>Environment Z</th>
</tr>
</thead>
</table>

Type: information, state report, disturbance
nr parameters, structure
operation, maintenance, stopped, emergency stop
return to normal. Value overrun, value underrun
plant object and sub-object

environment variables

The variable values are included when parsing the multi-lingual human-readable messages

"robot 5 on cell 31, motor 3 overheat (96°)." "robot 5 de cellule 31, moteur 3 surchauffe (96°)."
Trends allow to follow the behaviour of the plant and to monitor possible excursions. Monitored process data (sampled or event-driven) are stored in the historical database. Problem: size of the database (GB / month)
Historian

The historian keeps process relevant data at a lower granularity than the trend recorder, but with a larger quantity.

Data from different sources is aggregated in one data base, normally using data compression to keep storage costs low.

Data are analysed according to "calculation engines" to retrieve "metrics":
- performance indicators
- quality monitoring
- analysis of situations (why did batch A worked better than batch B)

Build the audit trail: "who did what, where and when"
especially in accordance with regulations (e.g. Food and Drugs Administration 's CFR 11)

Examples:
ABB's Information Manager
GE's iHistorian 2.0
Siemens's WinCC-Historian
Additional functions

printing logs and alarms (hard-copy)

reporting

display documentation and on-line help

email and SMS, voice, video (webcams)

access to databases (e.g. weather forecast)

optimisation functions

communication with other control centres

personal and production planning (can be on other workstations)
Special requirements for the food&drugs industry

The US Food&Drugs administration (FDA) requires a strict control of production for pharmaceuticals and food (FDA 21 CFR Part 11).

All process operations must be registered, the persons in charge known, the document signed (electronic signature), tamper-proof records kept.
Engineering tools

draw the objects
bind controllers to variables
define the reports and logs
define recipes (=macros)
distribute the SCADA application (on several computers, …)
support fault-tolerance and back-ups
define interfaces to external software (SQL, SAP, etc.)
Elements of the operator workstation

- mimic
- simulation
- instructor desk
- process data base
- actualisation
- process data
- plant
- state logging
- trend processing
- alarms processing
- alarms logging
- logging
Populating the Process Data Base

Process data represent the current state of the plant. Older values are irrelevant and are overwritten by new ones ("écrasées", überschrieben).

Process data are actualized either by
- polling (the screen fetches data regularly from the database (or from the devices))
- events (the devices send data that changed to the database, which triggers the screen)
Each station broadcasts cyclically all its variables: the control bus acts as an online database. Datasets are replicated by broadcast to any number of destinations.

Advantage: real-time response guaranteed.

Drawback: bus bandwidth may become insufficient with large number of urgent data.
Event-driven operation

Every PLC detects changes of state (events) and sends the new value over the bus. Each operator station receives and inserts data into its local database. Data are readily available for visualization. Multiple operator workstations could be addressed in multicast (acknowledged) or broadcast.

Drawback: consistency between databases, bus traffic peaks, delays.
To reduce bus traffic, the operator stations indicate to the controllers which data they need. The controllers only send the required data. The database is therefore moved to the controllers. The subscription can be replaced by a query (SQL) - this is ABB’s MasterNet solution.
Operator Interface

Operator Workstation design

Graphical User Interface **access** by Keyboard, Mouse, Trackball, Touch screen, Light pen

**display** of values, colours, shape depending on variable value

**operations** on visual objects (scaling, combination, events) and on acting objects (page change, sequence of events,..)

**navigation** from page to page (hierarchical, shortcuts, search,..)

- **I/O interface**
  - fieldbus
  - Ethernet

- **historical data base**
- **on-line data base**

- **DB optimised** for fast access (in RAM)

- **page layout**
- **page code**
- **page logic**

- **OPC**
- **Oracle**
- **dBase**
- **Access**
- **MS SQL**, ….
Example: Intellution's Fix32 internal structure

- C/C++ tasks
- VB tasks
- OBDC interface
- DDE interface

Draw

View

HTD
History & Trends

DBB
HTC
PDB

Printer Alarm Queue
File Alarm Queue
Historian Alarm Queue

SAC
(Alarm & Change)

raw process data

DIT

I/O driver

OPC
Scada SW architecture

- Field protocols: 101, 61850, HTTP
- Process data base
- OPC DA
- Data Acquisition
- Command language & procedures
- Remote Device Configuration
- FDT / DTM / XML
- Communication stream
- Measurand processing
- OPC AE
- Alarm & Event handling
- Application functions
- History data base
- ODBC/SQL
- Historian
- Reporting & Logging
- standards

Industrial Automation 32/40 5 Operator Interface
Model-Viewer-Controller: from E-commerce to Industry Operator Screen

browser on same or other machine (IE, Netscape, …)

web server (IIS, TomCat)

page logic code-behind (servlets, .NET)

data base

scripts & code (Java, Perl, C#, ..)

web-pages (HTM, JSP, ASP, ..)

the basic structure is the same….
...and why not simply Microsoft .NET?

The value of the visualization tools is not in the basic platform (which is often Microsoft, Java, .NET or similar) …

... it is in the conglomerate of tools and interface to different control systems they offer.

Some (Iconics) offer a library of ActiveX - Controls representing automation objects.

Protocols to a number of commercial PLCs are needed (ABB, Siemens, GE,…)

There is a growing similarity between products for SCADA and for E-commerce, but each is optimised for another market.
Why not Enterprise platform?

Figure 2. Confirming, selecting, and applying component units (Class chart by UML description).
An example of SCADA requirements

Action is based on production batches, signing in a new batch, identifying the paper material, filling good and responsible machine driver.

Connection to Mitsubishi A series and Siemens S7 PLCs, with asynchronous or Ethernet cable.

Connection to asynchronous ASCII-protocol communication devices for example F&P Bailey FillMag.

Process diagrams 4-5 pcs. including dynamic displays for valves and cylinders 40-50 pcs., motors 20 pcs., heaters 20 pcs., thermocouple-inputs 30-40 pcs.,

additional analog inputs 10 pcs.

Real time and historical trends 40-50 pcs.

Sequence displays including step-displays and clocks.

Alarm displays with additional help displays including text and pictures.

Parameter set displays for PID-controls, filling automates and servo drives.

Storing logged data to a transferable database.

quite different from E-commerce, but the platform could be the same…
## Generic visualization packages

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABB</td>
<td>Process Portal, OperatorIT</td>
</tr>
<tr>
<td>CTC Parker Automation</td>
<td>interact</td>
</tr>
<tr>
<td>Citect</td>
<td>CitectSCADA (AUS, ex CI technologies, <a href="http://www.citect.com">www.citect.com</a>)</td>
</tr>
<tr>
<td>Intellution (GE Fanuc)</td>
<td>Intellution (iFix3.0) 65000 installs, M$38 turnover</td>
</tr>
<tr>
<td>Iconics</td>
<td>Genesis</td>
</tr>
<tr>
<td>National Instruments</td>
<td>LabView, Lookout</td>
</tr>
<tr>
<td>Rockwell Software</td>
<td>RSView</td>
</tr>
<tr>
<td>Siemens</td>
<td>WinCC, ProTool/Pro</td>
</tr>
<tr>
<td>Taylor</td>
<td>Process Windows</td>
</tr>
<tr>
<td>TCP</td>
<td>SmartScreen</td>
</tr>
<tr>
<td>USDATA</td>
<td>Factorylink, 25000 installs, M$28 turnover</td>
</tr>
<tr>
<td>Wonderware (Invensys)</td>
<td>InTouch, 48000 installs, M$55 turnover</td>
</tr>
</tbody>
</table>

Manufacturing Execution System = MES
Pilotage de fabrication
Herstellungstechnik

Prof. Dr. H. Kirrmann
ABB Research Center, Baden, Switzerland
Manufacturing Execution System

MES is the intermediate layer (3) between Control (0,1,2) and Enterprise (4)

Source: ANSI/ISA–95.00.01–2000
Location of MES in the control hierarchy

MES: Integrated Production Data, Working with Operations Management Systems, People, And Practice

-source: MESA White Paper
Manufacturing model: Restaurant

- Accounting
- Menu
- Recipes
- Controller
- Cashier
- Chef
- Cooks
- Waiters
- Dish washer
- Suppliers
- Fresh food
- Prepared food
- Waste
- Clients
Type of production

make to stock

make to order

make to configuration
**Notions**

**Serial number:** a unique identifier assigned to a produced good, lot or part

**Bill of Material (BOM):** list of parts and consumables needed to produce a product

**Recipe:** the operations needed to produce a part

**Bill of Resources:** non consumable resources required for production

**Workflow:** the flow of parts within the factory

**Traceability:** ability to track where the parts a product come from and who assembled them

**Work Order:** order to produce a certain quantity of a product

**Push / pull:** produce when parts are available, require parts when product is required

**Kanban:** supplier cares that the parts tray of the client are never void.

**Scheduling / dispatching:** (flight timetable / tower) (Planer / Disponent)

**Engineering Change Order (ECO):** design or recipe errors reported to engineering.
Workflow is the path that the product being manufactured takes through several “stations”.

Recipe is the sequence of operations that takes place at one particular station.
**Office lay-outs impact order lead-time**

<table>
<thead>
<tr>
<th></th>
<th>Before</th>
<th>Current</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>11</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Distance</td>
<td>110 m</td>
<td>30 m</td>
<td>20 m</td>
</tr>
<tr>
<td>Time</td>
<td>70 hours</td>
<td>23 hours</td>
<td>7.5 hours</td>
</tr>
</tbody>
</table>

Before: ~ 300 meters (3 floors)  
Time: + 4 days

After: 9 meters  
Time: 2 hours
ISA S95 standard

This US standard defines terminology and good practices

- Delineate the business processes from the manufacturing processes
- Identify the responsibilities and functions in Business to Manufacturing and Manufacturing to Manufacturing integration
- Identify exchanged information in Business to Manufacturing integration
- Improve integration of manufacturing by defining:
  - Common terminology
  - Consistent set of models
- Establish common points for the integration of manufacturing systems with other enterprise systems
ANSI/ISA 95 standard documents

• ANSI/ISA95.00.01 “Enterprise - Control System Integration - Part 1: Models and Terminology”
  – Approved July 2000
  – IEC/ISO 62264-1 international standard approved and released by IEC/ISO

• ANSI/ISA95.00.02 “Enterprise - Control System Integration - Part 2: Data Structures and Attributes”
  – Approved October 2001
  – IEC/ISO 62264-2 international standard currently being reviewed by Joint Working Group

• Draft standards dS95.00.03 “Enterprise - Control System Integration - Part 3: Models of Manufacturing Operations”
  – Still under construction – Draft 14 released for review
Location hierarchy

- **Level 3 activities** typically deal with these objects:
  - process cell
  - production unit
  - production line
  - storage area
  - unit
  - work cell
  - storage unit
  - Lower level equipment used in batch operations
  - Lower level equipment used in continuous operations
  - Lower level equipment used in repetitive or discrete operations
  - Lower level equipment used in material management operations

- **Level 4 activities** typically deal with these objects:
  - enterprise
  - site
  - area
Location elements

Factory (plant)
Area
Production Line
Production Pool
Production Cell
Machine

- group of production cells with identical production capabilities
- a place where a particular manufacturing operation on the product is executed.
Production elements

Production

Lot

Product

a number of products of the same type to be manufactured as per production order, identified by a production ID

a number of products of the same type treated as a whole for a production

a final product, identified by its serial number

Part

identifiable components of the product, can be used for product tracking

Material

expendible, not individualized components of the product
A palette can carry a product or a lot.
Example: manufacturing steps for switchgears

- Cold Shrinked tube – Prepare the shrinked tubes by labelling cold shrinked tubes
- Assembly connector on top – assemble the connector on top of the 12 kV/24kV embedded poles, recording the torques.
- Assembly of high current EP – assemble, calculate quantity of washers, and record torque (only applies to high-current Eps)
- Epoxy Department – embed vacuum interrupter in epoxy in 4 steps: assembling connector to bottom, run the epoxy machinery, remove blur and analyse load number of resin
- Assembly of EP 12kV/24 kV assembly current strip and push rod, and record torques
- Testing - test continuous operation and voltage drops
- Assembly of push-rods – assembly according to part lists, spring force, and torque and generate barcode and print labels
Example: Assembly process

1. Vacuum Interrupter
2. Cold shrunked tube
3. Assembly connector on top
4. Epoxy department
5. Casted products
6. Assembly of EP 12 kV/24 kV
7. Connect push rod
8. Testing

Office, administration
Components
Prepared Embedded pole
Pre-heating
Assembly of connector on bottom
Casting
Finishing / post curing
Analysis
DSC
Buffer
Operation number
Operation / k place
Example: Plant for manufacturing switchgears
Dispatching and routing (workflow)
Workflow: Transportation, productivity and inventory waste ...

1. Tubes
2. Unprotected Cores
3. Protection
4. Taping
5. 2ry Winding
6. Short Circuit Test
7. Pre-Test
8. Protective Taping
9. Positioning
10. Buffer
11. 1ry Winding
12. Taping
13. Buffer

Order Travel
... have been vastly eliminated from the factory floor
Level 3: Manufacturing Execution System

dispatch and control the manufacturing process based on actual (“real-time”) data

recipe engineering

operation scheduling

documentation repository

resource allocation & status

labour management

dispatching production

process management

quality management

performance analysis

maintenance management

data collection & acquisition

product tracking & genealogy

product management

engineering

production tools

product

plant data

(ANSI/ISA 95 standard)
Manufacturing Workflow (e.g. pharmaceutical industry)
ISA S95: 1. Resource Allocation and Status

Guiding what people, machines, tools, and materials do, and what they are currently doing. Maintains and displays status of resources including machines, tools, labour, materials, etc. that must be available in order for work to start.

Detail

• manage **resources** (machines, tools, labour skills, materials, other equipment, documents, … that must be available for work to start and to be completed, directly associated with control and manufacturing.
• do local resource **reservation** to meet production-scheduling objectives.
• ensure that equipment is properly set up for processing, including any allocation needed for set-up.
• provide real-time **statuses** of the resources and a detailed history of resource use.
ISA S95: 2. Dispatching production (routing, workflow)

Giving commands to send materials or order to parts of the plant to begin a process or step.

Detail

• Manage the flow of production in the form of jobs, orders, batches, lots, and work orders, by dispatching production to specific equipment and personnel.

• Dispatch information is typically presented in the sequence in which the work needs to be done and may change in real time as events occur on the factory floor.

• Alter the prescribed schedules, within agreed upon limits, based on local availability and current conditions.

• Control the amount of work in process at any point through buffer management and management of rework and salvage processes.
ISA S95: 3. Data Collection

Monitoring, gathering, and organizing data about processes, materials, and operations from people, machines, or controls. Ability to collect and store data from production systems to use for population of forms and records. Data can be collected manually or automatically in real time increments.

Detail

- obtain the operational production and parametric data associated with the production equipment and processes.
- provide real-time status of equipment and production processes and a history of production and parametric data.
3. Data Collection Input devices specific for manufacturing

EAN Barcode

universal input device, serial number, error report.
Limited text length

Bar code label printer

Bar code scanner

PDF417: upcoming standard, high density coding
even small ink quantities may impair some products.
3. Data Collection RFIDs

RFID = Radio Frequency Identifiers

Hundreds or even thousands of tags can be identified at the same time at distance of 3m with a single reader antenna and 6m between two reader antennas.

At 13.56 MHz can store 512 bits, new versions working in the 915 MHz range
Price: 0.1 € / piece

Unsuitable on metal, high temperatures, - for the better and the worse.
3. Data Collection Local HMI

- Priority 1: 401298, LVD4
- Priority 2: 401299, LHD4/R

- Pole Configuration:
  - Control visually whether the type of the pole corresponds to the required one:
    - WS1 small pole
    - WS4 large pole with black ring
    - WS6 large pole with red ring
  - Configuration checked:

- Pallet Identification:
  - Support Tool ID: 200
  - Serial Number: A0000A6280

- Supervisor Message

- Bill Of Material

- Safety
ISA S95: 4. Quality Management

Recording, tracking and analyzing product/process characteristics against engineering needs.

Detail

• provide real-time measurements collected from manufacturing and analysis in order to assure proper product quality control and to identify problems requiring attention.

• Recommend corrections, including correlating the symptoms, actions and results to determine the cause.

• **SPC/SQC** (statistical process control/statistical quality control) tracking and management of offline inspection operations and analysis in laboratory information management systems (LIMS).
4: Quality Test

ABBE DISTRIBUTION AUTOMATION EQUIPMENT DIVISION
LAKE MARY, FLORIDA
CERTIFIED TEST REPORT - RETROFIT CABINETS

GENERAL ORDER #__________________  SHOP ORDER__________________

UNIT SERIAL # ____________________ CUSTOMER # ______________________

PCD STYLE #________________________ PCD SERIAL # ________________

SOFTWARE VERSION NUMBER ________________________________________

FRONT PANEL CONTROLS
A. REMOTE ENABLE______________ OK
B. GROUND BLOCK_______________ OK
C. ALTERNATE PU_______________ OK
D. SEF ENABLE________________ OK
E. RECLOSE BLOCK______________ OK
F. PROG. 1______________________ OK (BATTERY TEST)
G. FAULT TEST__________________ OK (SELF TEST)

CONTROL FUNCTIONS
A. MINIMUM PICKUP, PHASE 1____OK  PHASE 2 ___OK  PHASE 3 ___OK  GROUND ____OK
B. INSTANTANEOUS TRIPPING____OK
C. TIME DELAY TRIPPING_______OK
D. RECLOSE TIMES_______OK
E. RESET TIME_____OK

INPUT/OUTPUT TEST
INTERLOCKED WITH REMOTE ENABLED FUNCTION
REMOTE CLOSE______________ OK
REMOTE TRIP______________ OK
REMOTE RECLOSE BLOCK_____ OK
REMOTE ALT. 1______________ OK

INDEPENDENT OF REMOTE ENABLE FUNCTION
SUPERVISOR CLOSE_________ OK
SUPERVISORY TRIP___________ OK
VOLTAGE WITHSTAND

CHECK THE CONTROL CABINET WIRING, TO GROUND, AT 1500 VAC FOR

Typical Final Inspection Checklist
4: Example of quality statistics

X-bar and R Chart; variable: **HEIGHT of Stator**

**Histogram of Means**
X-bar: 780.71 (780.71); Sigma: 2.2978 (2.2978); n: 4.

**Histogram of Ranges**
Range: 4.7306 (4.7306); Sigma: 2.0216 (2.0216); n: 4.
ISA S95: 5. Process Management

Directing the flow of work in the plant based on planned and actual production activities.

Detail

• monitor production and either automatically corrects or provides decision support to operators for correcting and improving in-process functions. These functions may be intra-operational and focus specifically on machines or equipment being monitored and controlled, as well as inter-operational, tracking the process from one operation to the next.

• manage alarms to ensure factory persons are aware of process changes that are outside acceptable tolerances.
ISA S95: 6. Product Tracking & Genealogy

Monitoring the progress of units, batches, or lots of output to create a full product history.

Detail

• Monitors and tracks material used in a manufactured part including revisions, sources, serial numbers, supplier identification, or lot. This information is retrievable in the event of quality problems or process changes to identify comparable products.

• record information to allow forward and backward traceability of components and their use within each end product.
ISA S95: 7. Performance Analysis

Comparing measured results in the plant to goals and metrics.

Ability to consolidate collected data and calculate results including real production cost, uptime, SPC/SQC of production parts, etc. Includes comparison of current vs. historical performance.

Detail

• Provide up-to-the-minute reporting of actual manufacturing operations results along with comparisons to past history and expected results.

• Performance results include such measurements as resource utilization, resource availability, product unit cycle time, conformance to schedule, and performance to standards.

• Include SPC/SQC analysis and may draw from information gathered by different control functions that measure operating parameters.
7. Performance Analysis: questions the factory owner asks

What is the number of good / bad pieces produced: by shift X, in week 20?
(with / without induced downtime)
What is the relation to the maximum?

What was the average production speed of a unit compared to the maximum?
What is the production speed in function of time, deducing stops?

How much afar from the theoretical production capacity is my plant producing?

What are the N major reasons why the unit is not producing at full capacity?
How many stops did the unit suffered?

What is the availability of my production unit

What is the efficiency of operator M ?, of shift S ?

What is the progression of the OEE (overall equipment efficiency) on a daily basis?
How much time is spent loading / unloading the machine?

How does my OEE compares with others?
7. Performance analysis and Pareto

![Performance Analysis Diagram](image-url)
ISA S95: 8. Operations and detailed scheduling

Sequencing and timing activities for optimised plant performance based on finite capacities of the resources

Detail

- Provide sequencing based on priorities, attributes, characteristics, and production rules associated with specific production equipment and specific product characteristics, such as shape, colour sequencing or other characteristics that, when scheduled in sequence properly, minimize set-up.

- Operations and detailed scheduling is finite and it recognizes alternative and overlapping/parallel operations in order to calculate in detail the exact time of equipment loading and adjustment to shift patterns.
ISA S95: 9 Document Control

Managing and distributing information on products, processes, designs, or orders. Controls records and forms that must be maintained to serve regulatory and quality needs and populates those forms with actual production data.

Also maintains current documents provided to operators to assist in production methods.

Detail:

- control records and forms that must be maintained with the production unit. (records and forms include work instructions, recipes, drawings, standard operation procedures, part programs, batch records, engineering change notices, shift-to-shift communication, as well as the ability to edit "as planned" and "as built" information).

- send instructions down to the operations, including providing data to operators or recipes to device controls.

- control and integrity of regulatory, documentation, environmental, health and safety regulations, and operative information such as corrective action procedures.
SA S95: 10 Labour Management

Tracking and directing the use of operations personnel based on qualifications, work patterns and business needs

detail

- provide status of personnel in an up-to-the minute time frame.
- provide time and attendance reporting, certification tracking,
- track indirect functions such as material preparation or tool room work as a basis for activity-based costing.
- interact with resource allocation to determine optimal assignments.
ISA S95: 11. Maintenance Management

Planning and executing activities to keep capital assets in the plant performing to goal.

**Detail**

- Maintain equipment and tools.
- Ensure the equipment and tools availability for manufacturing.
- Schedule periodic or preventive maintenance as well as responding to immediate problems.
- Maintain a history of past events or problems to aid in diagnosing problems.
Additional definitions

12. Work order tracking (not S95)
Directing the flow of work in the plant based on planned and actual production activities
Monitors work orders as they pass through the operations. Real time status provides management with view of actual production output and permits workflow changes based on business rules.

13. Recipe Manager: (not S95)
Mapping production order operations to detailed list of tasks/jobs, providing detailed recipe for manufacturing
Conclusion

MES is a business of its own, that require a good knowledge of the manufacturing process and organization skills.

Simulation tools are helpful to anticipate the real plant behavior.

Although buzzwords abound ("lean manufacturing", …), it is more an issue of common sense than of science.
Assessment

Which are the parts of the ISA S95 standard?

What does Kanban mean?

What is asset management?

Which manufacturing models exist?

What is a KPI and which KPI is a client interested in?

Which level 1 plants does ISA S95 consider?
Real-time consideration

Considération du temps réel
Echtzeit - Berücksichtigung

Prof. Dr. H. Kirrmann
ABB Research Center, Baden, Switzerland
Real-time constraints

Marketing calls "real-time" anything "fast", "actual" or "on-line"

Definition: A real-time control system is required to produce output variables that respect defined time constraints.

Levels of real-time requirements:
- meet all time constraints exactly (hard real-time)
- meet timing constraints most of the time (soft real-time)
- meet some timing constraints exactly and others mostly.

These constraints must be met also under certain error conditions

Effects of delays
- In regulation tasks, delays of the computer appear as dead times, which additionally may be affected by jitter (variable delay).
- In sequential tasks, delays slow down plant operation, possibly beyond what the plant may tolerate.
**Reaction times**

10 µs: positioning of cylinder in offset printing (0.1 mm at 20 m/s)

46 µs: sensor synchronization in bus-bar protection for substations (1° @ 60Hz)

100 µs: resolution of clock for a high-speed vehicle (1 m at 360 km/h)

100 µs: resolution of events in an electrical grid

1.6 ms: sampling rate for protection algorithms in a substation

10 ms: resolution of events in the processing industry

20 ms: time to close or open a high current breaker

200 ms: acceptable reaction to an operator's command (hard-wire feel)

1 s: acceptable refresh rate for the data on the operator's screen

3 s: acceptable set-up time for a new picture on the operator's screen

10 s: acceptable recovery time in case of breakdown of the supervisory computer

1 min: general query for refreshing the process data base in case of major crash
Processing times

1 µs: addition of two variables in a programmable logic controller
10 µs: execution of an iteration step for a PID control algorithm.
30 µs: back- and forth delay in a 3'000 m long communication line.
40 µs: coroutine (thread) switch within a process
160 µs: send a request and receive an immediate answer in a field bus
100 µs: task switch in a real-time kernel
200 µs: access an object in a fast process database (in RAM)
1 ms: execution of a basic communication function between tasks
2 ms: sending a datagram through a local area network (without arbitration)
16 ms: cycle time of a field bus (refresh rate for periodic data)
60 ms: cycle time of the communication task in a programmable logic controller.
120 ms: execution of a remote procedure call (DCOM, CORBA).
What real-time response really means

The operator keeps one hand on the “rotate” button while he washes with the other. If the towel gets caught, he releases the button and expects the cylinder to stop in 1/2 second ...
The signal path from the emergency stop to the motor

Main controller (processing every 30 ms)

IBS (2 ms, 500 kb/s)

Display

Lokalbus

BA DIO MCU LBA

IBS-M

emergency button

tower bus (1.5 Mbit/s, 32 ms)

Safety controller

IBS-S

IBS (2 ms, 500 kb/s)

BA AIO MCU LBA

tower control

Motor control

IBS-S

processing every 40 ms

section control

section bus (1.5 Mbit/s, 32 ms)

processing every 40 ms

Motor control

SERCOS ring (4 ms)

Total delay path: 2 + 30 + 32 + 40 + 32 + 40 + 4 = 180 ms!
Delay path and reaction time

Most safety systems operate negatively:
-> lack of “ok” signal (life-sign toggle) triggers emergency shutdown

The motor control expects that the information “emergency button not pressed” is refreshed every $3 \times 180 = 540$ ms to deal with two successive transmission errors, otherwise it brakes the motors to standstill.

Excessive signal delay causes false alarms -> affects availability of the plant (client won’t accept more than 1-2 emergency shutdown due to false alarm per year)

Therefore, control of signal delays is important:
- for safety
- for availability
8 Real-time considerations

### Hard- and Soft real time

**Hard real-time** (deterministic)
- **Probability**
- **Deadline**
- **Bound!**

- The probability of the delay to exceed an arbitrary value is zero under normal operating conditions, including recovery from error conditions.

**Soft real-time** (non-deterministic)
- **Probability**
- **Deadline**
- **Unbound!**

- The probability of the delay to exceed an arbitrary value is small, but non-zero under normal operating conditions, including recovery from error conditions.
Hard Real-Time and Soft Real-Time: series connection

Hard real-time (cyclic)

Soft real-time (event-driven, CSMA)

1 element

2 elements in series

probability of two elements in series = convolution integral

delay

bound!

probability

t1 tA t2

t1 + t3 tA t2 + t4

t1 t3 t2 t4

still bound!

unbound!

unbound!

probability in the order of $10^{-6} = 1$ transmission failure per
# Determinism and transmission failures

<table>
<thead>
<tr>
<th>Individual period</th>
<th>Individual period</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Diagram" /></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
</tbody>
</table>

- **Bus master**
- **1 2 3 4 5 6**

- **Probability**
- **Response time**

- **No more data expected after** $T_{CD}$

- **(heaps are exaggerated)**
- **Contingency deadline, e.g. emergency shutdown**

Example: probability of data loss per period = 0.001,
probability of not meeting $T_{CD}$ after three trials = $10^{-9}$,
same order of magnitude as hardware errors -> emergency action is justified.
Deterministic systems

A deterministic system will react within bound delay under all conditions.

A deterministic system can be defeated by external causes (failure of a device, severing of communication line), but this is considered as an accepted exceptional situation for which reaction is foreseen.

Determinism implies previous reservation of all resources (bus, memory space,...) needed to complete the task timely.

All elements of the chain from the sensor to the actor must be deterministic for the whole to behave deterministically.

Non-deterministic components may be used, provided they are properly encapsulated, so their non-determinism does not appear anymore to their user.

Examples:
• queues may be used provided:
  a high-level algorithm observed by all producers ensures that the queues never contains more than N items.
• Interrupts may be used provided:
  the interrupt handler is so short that it may not cause the interrupted task to miss its deadline, the frequency of interrupts being bound by other rules (e.g. a task has to poll the interrupts)
Deterministic Control Systems

For real-time systems, small, affordable and well-understood kernels are used: VRTX, VxWorks, RTOS, etc....

The tasks in these systems normally operate cyclically, but leave room for event processing when idle - the cyclic task must always be able to resume on time.

Control network does not depend on raw speed, but on response time.

Control loops need timely transmission of all critical variables to all sink applications.

- If an application sends one variable in 7 ms to another application, transmission of all variables may require \( n \times 7 \) ms (except if several variables are packed in one message).

- If several applications are interested in a variable, the number of transfer increases, except if transmission is (unacknowledged) broadcast.

Smooth execution of control algorithms require that data are never obsolete by more than a certain amount.

Determinism is closely related to the principle of cyclic operation.
Non-deterministic systems

A non-deterministic system can fail to meet its deadline because of internal causes (congestion, waiting on resource), without any external cause.

Computers and communication may introduce non-deterministic delays, due to internal and external causes:
- response to asynchronous events from the outside world (interrupts)
- access to shared resources: computing power, memory, network driver, ...
- use of devices with non-deterministic behavior (hard-disk sector position)

Non-determinism is especially caused by:

- Operating system with preemptive scheduling (UNIX, Windows,..) or virtual memory (in addition, their scheduling algorithm is not parametrizable)
- Programming languages with garbage collection (Java, C#, ...)
- Communication systems using a shared medium with collision (Ethernet)
- Queues for access to the network (ports, sockets)

Non-determinism is closely related to on-demand (event-driven) operation
Failures in Ethernet - Style transmission

multi-master bus with CSMA

Probability of transmission failure due to collision: e.g. 1% (generous)
(Note: data loss due to collision is much higher than due to noise !)

With no collision detection, retransmission is triggered by not receiving acknowledgement of remote party within a time $T_{rto}$ (reply time-out).

This time must be larger than the double queue length at the sender and at the receiver, taking into account bus traffic. Order of magnitude: 100 ms.

The probability of missing three $T_{rto}$ in series is $G^3$ times larger than a cyclic system with a period of 100 ms, $G$ being the ratio of failures caused by noise to failures caused by collisions (here: 1% vs. 0.01% -> $10^6$ more emergency stops.)
Case study: Analysis of the response of an event-driven control system

Typical stress situation: loss of power

Binary variables: event is a change of state

Analog variables: event is a change of value by more than 0.5 %
Solution 1: PLC attach to plant through Field Bus

Up to 40 Operator Workstation 1000 events/s each

Ethernet 12'500 events/s @ 10% load

up to 6 PLC 300 events/s each

Field Busses 60 µs/16bit = 16'666 data /s

Total : 15'900 samples/s

Analog inputs: 2200 @ 1s, 300 @ 0.1 s = 5200 /s
Binary inputs: 2700 @ 1s, 300 @ 0.1 s = 5700 /s
Binary stamped inputs: 1000 @ 1s, 400 @ 0.1 s = 5000 /s
Solution 2: OWS access Field Bus and PLCs directly

Operator Workstation
1000 events/s each

duplicated Ethernet
12500 events/s @ 10% load)

field bus
60 µs/16bit
= 16'666 data /s

8 Real-time considerations
The analysis of the delay distribution in all possible cases requires a complete knowledge of the plant and of the events which affect the plant.

It is not only event transmission which takes time, but also further processing...
What is the worst-case condition?

Every second, 15'900 variables are sampled, but most of them do not change and do not give rise to an event. Since events are spread evenly over the DDS, no queue builds up as long as the event rate does not pass 286 per second.

Worst case situation: loss of secondary power.

2500 binary events occur in the first second, but few in the following seconds. With automatic reconnection, a second peak can occur. The analog avalanche causes about 100 changes in the first 2 seconds and 40 in the following 40 seconds:

binary and analog avalanches:
Where is the bottleneck?

It can take up to 7 s until the avalanche is absorbed, i.e. until the operator has access to any particular variable.

Even in the worst case, the communication load over the Ethernet does not present a problem, since the production of events by the devices cannot exceed 1/15 ms, representing 0.33 % of the Ethernet's bandwidth.

The bottleneck was not the Ethernet capacity as was assumed, but the insufficient processing power of the operator workstations....
Always consider the whole system....
Conclusions

- Determinism is a basic property required of a critical control and protection system. A non-deterministic system is a "fair-weather" solution.

- A deterministic control system guarantees that all critical data are delivered within a fixed interval of time, or not at all.

- A deterministic system operates in normal time under worst-case conditions - this implies that resources seem wasted.

- The whole path from application to application (production, transmission and processing) must be deterministic, it is not sufficient that e.g. the medium access be deterministic.

- One can prove correctness of a deterministic system, but one cannot prove that a non-deterministic system is correct.

- Any non-deterministic delay in the path requires performance analysis to prove that it would work with a certain probability under realistic stress conditions.
Assessment

1 What is the difference between soft and hard real-time?

2 What does determinism mean and what does it allow to assess?

3 What is to be done when non-deterministic components are present?

4 What are the advantages and disadvantages of event-driven vs. cyclic systems?

5 Can the response time of a hard real-time system be exactly predicted?

5 Under which conditions can non-deterministic components be used?
9.1 Dependability - Overview
Sûreté de fonctionnement - Vue d’ensemble
Verlässlichkeit - Übersicht

Prof. Dr. H. Kirrmann & Dr. B. Eschermann
ABB Research Center, Baden, Switzerland
Control Systems Dependability

9.1: Overview Dependable Systems
   - Definitions: Reliability, Safety, Availability etc.,
   - Failure modes in computers

9.2: Dependability Analysis
   - Combinatorial analysis
   - Markov models

9.3: Dependable Communication
   - Error detection: Coding and Time Stamping
   - Persistency

9.4: Dependable Architectures
   - Fault detection
   - Redundant Hardware, Recovery

9.5: Dependable Software
   - Fault Detection,
   - Recovery Blocks, Diversity

9.6: Safety analysis
   - Qualitative Evaluation (FMEA, FTA)
   - Examples
Motivation for Dependable Systems

Systems - if not working properly in a particular situation - may cause
- large losses of property or money
- injuries or deaths of people

To avoid such effects, these “mission-critical” systems must be designed specially so as to achieve a given behaviour in case of failure.

The necessary precautions depend on
- the probability that the system is not working properly
- the consequences of a system failure
- the risk of occurrence of a dangerous situation
- the negative impact of an accident (severity of damage, money lost)
Application areas for dependable systems

Space Applications
- Launch rockets, Shuttle, Satellites, Space probes

Transportation
- Airplanes (fly-by-wire), Railway signalling, Traffic control, Cars (ABS, ESP, brake-by-wire, steer-by-wire)

Nuclear Applications
- Nuclear power plants, Nuclear weapons, Atomic-powered ships and submarines

Networks
- Telecommunication networks, Power transmission networks, Pipelines

Business
- Electronic stock exchange, Electronic banking, Data stores for Indispensable business data

Medicine
- Irradiation equipment, Life support equipment

Industrial Processes
- Critical chemical reactions, Drugs, Food
Market for safety- and critical control systems

Increases more rapidly than the rest of the automation market

Source: ARC Advisory group, 2002, Asish Ghosh
Definitions: Failure, Fault

A *mission* is the intended (specified) function of a device.

A *failure* (*Ausfall*, *défaillance*) is the non-fulfilment of this mission.

("termination of the ability of an item to perform its required function").

failures may be:

- momentary = outage (*Aussetzen*, *raté*)
- temporary = need repair = breakdown (*Panne*, *panne*) - for repairable systems only -
- definitive = (*Misserfolg*, *échec*)

A *fault* (*Fehler*, *défaut*) is the cause of a failure, it may occur long before the failure.

These terms can be applied to the whole system, or to elements thereof.
Fault, Error, Failure

Fault: missing or wrong functionality
  – permanent: due to irreversible change, consistent wrong functionality (e.g. short circuit between 2 lines)
  – intermittent: sometimes wrong functionality, recurring (e.g. loose contact)
  – transient: due to environment, reversible if environment changes (e.g. electromagnetic interference)

Error: logical manifestation of a fault in an application (e.g. short circuit leads to computation error if 2 lines carry different signals)

Failure: to perform a prescribed function (e.g. if different signals on both lines lead to wrong output of chip)

\[ \text{fault} \xrightarrow{\text{may cause}} \text{error} \xrightarrow{\text{may cause}} \text{failure} \]
Hierarchy of Faults/Failures

- **Component level**: e.g., transistor short circuited
- **Subsystem level**: e.g., memory chip defect
- **System level**: e.g., computer delivers wrong outputs
Types of Faults

Computers can be affected by two kinds of faults:

- **physical faults** (e.g. hardware faults)
  - "a corrected physical fault can occur again with the same probability."
- **design faults** (e.g. software faults)
  - "a corrected design error does not occur anymore"

Faults are originated by other faults (causality chain).

Physical faults can originate in design faults (e.g. missing cooling fan)

Most work in fault-tolerant computing addresses the physical faults, because it is easy to provide redundancy for the hardware elements.

Redundancy of the design means that several designs are available.
Random and Systematic Errors

Systematic errors are reproducible under given input conditions
Random Error appear with no visible pattern.

Although random errors are often associated with hardware errors and
systematic errors with software errors, this needs not be the case

Transient errors, firm errors, soft errors, ..., do not use these terms
Example: Sources of Failures in a telephone exchange

- Software: 35%
- Hardware: 20%
- Handling: 30%
- Unsuccessful recovery: 15%

source: Troy, ESS1 (Bell USA)
Basic concepts
Reliability and Availability

**Definition:**

Reliability: "probability that an item will perform its required function in the specified manner and under specified or assumed conditions over a given time period"

Expressed shortly by its MTTF: Mean Time To Fail

Availability: "probability that an item will perform its required function in the specified manner and under specified or assumed conditions at a given time"
Failure/Repair Cycle

Without repair:

- \text{system works} \quad \text{system no longer works}

- \text{MTTF: mean time to fail}

With repair:

- \text{system works} \quad \text{down} \quad \text{system works}

- \text{MUT (MTTF)} \quad \text{MDT (MTTR)} \quad \text{MUT} \quad \text{MDT}

- \text{MTBF: mean time between failures, ("n'est pas "moyenne des temps de bon fonctionnement")}

\text{MTBF} = \text{MTTF} + \text{MTTR}

\text{if MTTR \ll MTTF: MTBF \approx MTTF}
**Redundancy**

Increasing safety or availability requires the introduction of redundancy (resources which are not needed if there were no failures).

Faults are detected by introducing a **check redundancy**.

Operation is continued thanks to **operational redundancy** (can do the same task)

Increasing reliability and maintenance quality increases both safety and availability.

- switch to red: no accident risk (safe)
  decreased traffic performance

- switch to green: accident risk traffic continues (available)
Availability and Repair in redundant systems

When redundancy is available, the system does not fail until redundancy is exhausted (or redundancy switchover is unsuccessful)
**Maintenance**

"The combination of all technical and administrative actions, including supervision actions intended to retain a component in, or restore it to, a state in which it can perform its required function"

Maintenance takes the form of

- **corrective maintenance**: executed when a part actually fails (repair)
  "go to the garage when the motor fails"

- **preventive maintenance**: restoring redundancy
  and in particular restore degraded parts to error-free state
  "go to the garage to change oil and pump up the reserve tyre"

- **scheduled maintenance** (time-based maintenance)
  "go to the garage every year"

- **predictive maintenance** (condition-based maintenance)
  "go to the garage at the next opportunity since motor heats up"

preventive maintenance does not necessarily stop production if redundancy is available
"differed maintenance" is performed in a non-productive time.
Redundancy does not replace maintenance: it allows to differ maintenance to a convenient moment (e.g. between 02h00 and 04h00 in the morning).

The system may remain on-line or be taken shortly out of operation.

The mean time between repairs (MTBR) expressed how often any component fails.

The mean time between failure concerns the whole system.

Differed maintenance is only interesting for plants that are not fully operational 24/24.
Preventive maintenance

In principle, preventive maintenance restores the initially good state at regular intervals.

This assumes that the coverage of the tests is 100% and that no uncorrected aging takes place.
Safety

we distinguish:

• hazards caused by the presence of control system itself:
  explosion-proof design of measurement and control equipment
  (e.g. Ex-proof devices, see "Instrumentation")

• implementation of safety regulation (protection) by control systems
  "safety"- PLC, "safety" switches
  (requires tamper-proof design)
  protection systems in the large
  (e.g. Stamping Press Control (*Pressesteuerungen*),
  Burner Control (*Feuerungssteuerungen*)

• hazard directly caused by malfunction of the control system
  (e.g. flight control)
Safety

The probability that the system does not behave in a way considered as dangerous.

Expressed by the probability that the system does not enter a state defined as dangerous.
Safe States

Safe state
- exists: sensitive system
- does not exist: critical system

Sensitive systems
- railway: train stops, all signals red (but: fire in tunnel?)
- nuclear power station: switch off chain reaction by removing moderator (may depend on how reactor is constructed)

Critical systems
- military airplanes: only possible to fly with computer control system (plane inherently instable)
Types of Redundancy

Structural redundancy (hardware):
Extend system with additional components that are not necessary to achieve the required functionality (e.g. overdimension wire gauge, use 2-out-of-3 computers)

Functional redundancy (software):
Extend the system with unnecessary functions
   – additional functions (e.g. for error detection or to switch to standby unit)
   – diversity (additional different implementation of the required functions)

Information redundancy:
Encode data with more bits than necessary
(e.g. parity bit, CRC, 1-out-of-n-code)

Time redundancy:
Use additional time, e.g. to do checks or to repeat computation
### Availability and Safety (1)

<table>
<thead>
<tr>
<th>Availability</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>availability is an economical objective.</td>
<td>safety is a regulatory objective</td>
</tr>
<tr>
<td>high availability increases production time and yield (e.g. airplanes are aloft)</td>
<td>high safety reduces the risk to the process and its environment</td>
</tr>
<tr>
<td>The gain can be measured in additional up-time</td>
<td>The gain can be measured in lower insurance rates</td>
</tr>
<tr>
<td>availability depends on a functional redundancy (which can take over the function) and on the quality of maintenance</td>
<td>safety depends on the introduction of check redundancy (fail-stop systems) and/or functional redundancy (fail-operate systems)</td>
</tr>
</tbody>
</table>

Safety and Availability are often contradictory (completely safe systems are unavailable) since they share redundancy.
Cost of failure in function of duration

losses (US$)

1. grace
2. detection
3. trip
4. damage

 damages
 protection
 trip
 protection does not trip

T_{grace} T_{detect} T_{trip} T_{damage}

stand-still costs

time
Safety and Security

Safety (Sécurité, Sicherheit):

Avoid dangerous situations due to unintentional failures
- failures due to random/physical faults
- failures due to systematic/design faults

  e.g. railway accident due to burnt out red signal lamp
  e.g. rocket explosion due to untested software (→ Ariane 5)

Security (Sécurité informatique, IT-Sicherheit):

Avoid dangerous situations due to malicious threats
- authenticity / integrity (intégrité): protection against tampering and forging
- privacy / secrecy (confidentialité, Vertraulichkeit): protection against eavesdropping

  e.g. robbing of money tellers by using weakness in software
  e.g. competitors reading production data

The boundary is fuzzy since some unintentional faults can behave maliciously.

(Sûreté: terme général: aussi probabilité de bon fonctionnement, Verlässlichkeit)
How to Increase Dependability?

Fault tolerance: Overcome faults without human intervention.

Requires **redundancy**: Resources normally not needed to perform the required function.
Check Redundancy (that can detect incorrect work)
Functional Redundancy (that can do the work)

Contradiction: Fault-tolerance increases complexity and failure rate of the system.

Fault-tolerance is no panacea: Improvements in dependability are in the range of 10..100.

Fault-tolerance is costly:
- x 3 for a safe system,
- x 4 times for an available 1oo2 system (1-out-of-2),
- x 6 times for a 2oo3 (2-out-of-3) voting system

**Fault-tolerance is no substitute for quality**
Dependability

(Sûreté de fonctionnement, Verlässlichkeit)

goals
- reliability
- availability
- maintainability
- safety
- security

achieved by
- fault avoidance
- fault detection/diagnosis
- fault tolerance
  (= error avoidance)

by error passivation
- fault isolation
- reconfiguration
  (on-line repair)

by error recovery
- forward recovery
- backward recovery

by error compensation
- fault masking
- error correction

guaranteed by
- quantitative analysis
- qualitative analysis
**Failure modes in computers**

9.1: Overview Dependable Systems
   - Definitions: Reliability, Safety, Availability etc.,
   - *Failure modes in computers*

9.2: Dependability Analysis
   - Combinatorial analysis
   - Markov models

9.3: Dependable Communication
   - Error detection: Coding and Time Stamping
   - Persistency

9.4: Dependable Architectures
   - Fault detection
   - Redundant Hardware, Recovery

9.5: Dependable Software
   - Fault Detection,
   - Recovery Blocks, Diversity

9.6: Safety analysis
   - Qualitative Evaluation (FMEA, FTA)
   - Examples
Failure modes in computers

Safety or availability can only be evaluated considering the total system controller + plant.
Computers and Processes

Availability/safety depends on output of computer system and process/environment.
Types of Computer Failures

Computers can fail in a number of ways

Breach of the specifications = does not behave as intended

reduced to two cases

output of wrong data
or of correct data, but at undue time

integrity breach

missing output of correct data

persistence breach

Fault-tolerant computers allow to overcome these situations.

The architecture of the fault-tolerant computer depends on the encompassed dependability goals
Safety Threats

depending on the controlled process,
safety can be threatened by failures of the control system:

**integrity breach**

not recognized, wrong data, or correct data, but at the wrong time

if the process is irreversible
(e.g. closing a high power breaker, banking transaction)

Requirement:
fail-silent (fail-safe, fail-stop) computer
"rather stop than fail"

**persistency breach**

no usable data, loss of control

if the process has no safe side
(e.g. landing aircraft)

Requirement:
fail-operate computer
"rather some wrong data than none"

Safety depends on the tolerance of the process against failure of the control system.
Plant type and dependability

**continuous systems**

modelled by differential equations, and in the linear case, by Laplace or z-transform (sampled)

![Graph showing F(nT) over time](image)

continuous systems are generally reversible.

tolerates sporadic, wrong inputs during a limited time (similar: noise)

tolerate loss of control only during a short time.

require persistent control

**discrete systems**

modelled by state machines, Petri nets, Grafcet,....

transitions between states are normally irreversible.

do not tolerate wrong input.
difficult recovery procedure

tolerate loss of control during a relatively long time (remaining in the same state is in general safe).

require integer control
## Persistency/Integrity by Application Examples

<table>
<thead>
<tr>
<th>secondary system</th>
<th>primary system</th>
<th>availability</th>
<th>safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>integrity</td>
<td></td>
<td>substation protection</td>
<td>railway signalling</td>
</tr>
<tr>
<td>persistency</td>
<td></td>
<td></td>
<td>airplane control</td>
</tr>
</tbody>
</table>
Protection and Control Systems

Control system:
Continuous non-stop operation
(open or closed loop control)
Maximal failure rate given in failures per hour.

Protection system:
Not acting normally, forces safe state (trip) if necessary
Maximal failure rate given in failures per demand.

[Diagram showing control, process, measurement, and protection systems]
Example Protection Systems: High-Voltage Transmission

Two kinds of malfunctions:
An underfunction (not working when it should) of a protection system is a safety threat
An overfunction (working when it should not) of a protection system is an availability threat
Findings

Reliability and fault tolerance must be considered early in the development process, they can hardly be increased afterwards.

Reliability is closely related to the concept of quality, its root are laid in the design process, starting with the requirement specs, and accompanying through all its lifetime.
References

H. Nussbaumer: Informatique industrielle IV; PPUR.
J.-C. Laprie (ed.): Dependable computing and fault tolerant systems; Springer.
J.-C. Laprie (ed.): Guide de la sûreté de fonctionnement; Cépaduès.
D. Siewiorek, R. Swartz: The theory and practice of reliable system design; Digital Press.
T. Anderson, P. Lee: Fault tolerance - Principles and practice; Prentice-Hall.
A. Birolini: Quality and reliability of technical systems; Springer.
M. Lyu (ed.): Software fault tolerance: Wiley.

Conferences: International Conference on Dependable Systems and Networks, European Dependable Computing Conference
Assessment

which kinds of fault exist and how are they distinguished

explain the difference between reliability, availability, safety in terms of a state diagram

explain the trade-off between availability and safety

what is the difference between safety and security

explain the terms MTTF, MTTR, MTBF, MTBR

how does a protection system differ from a control system when considering failures?

which forms of redundancy exist for computers?

how does the type of plant influence its behaviour towards faults?