MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

Industrial Automation (ICE 3252)

Distributed Control Systems

Bipin Krishna
Assistant Professor (Sr.)
ICE Department
Manipal Institute of Technology
MAHE, Karnataka, India

Introduction:

- The term DCS stands for Distributed Control System.
- They used to be referred to as distributed digital control systems (DDCS) earlier, implying that all DCS are digital control systems.
- They use digital encoding and transmission of process information and commands.
- DCS are deployed today not only for all advanced control strategies but also for the low-level control loops.

Introduction:

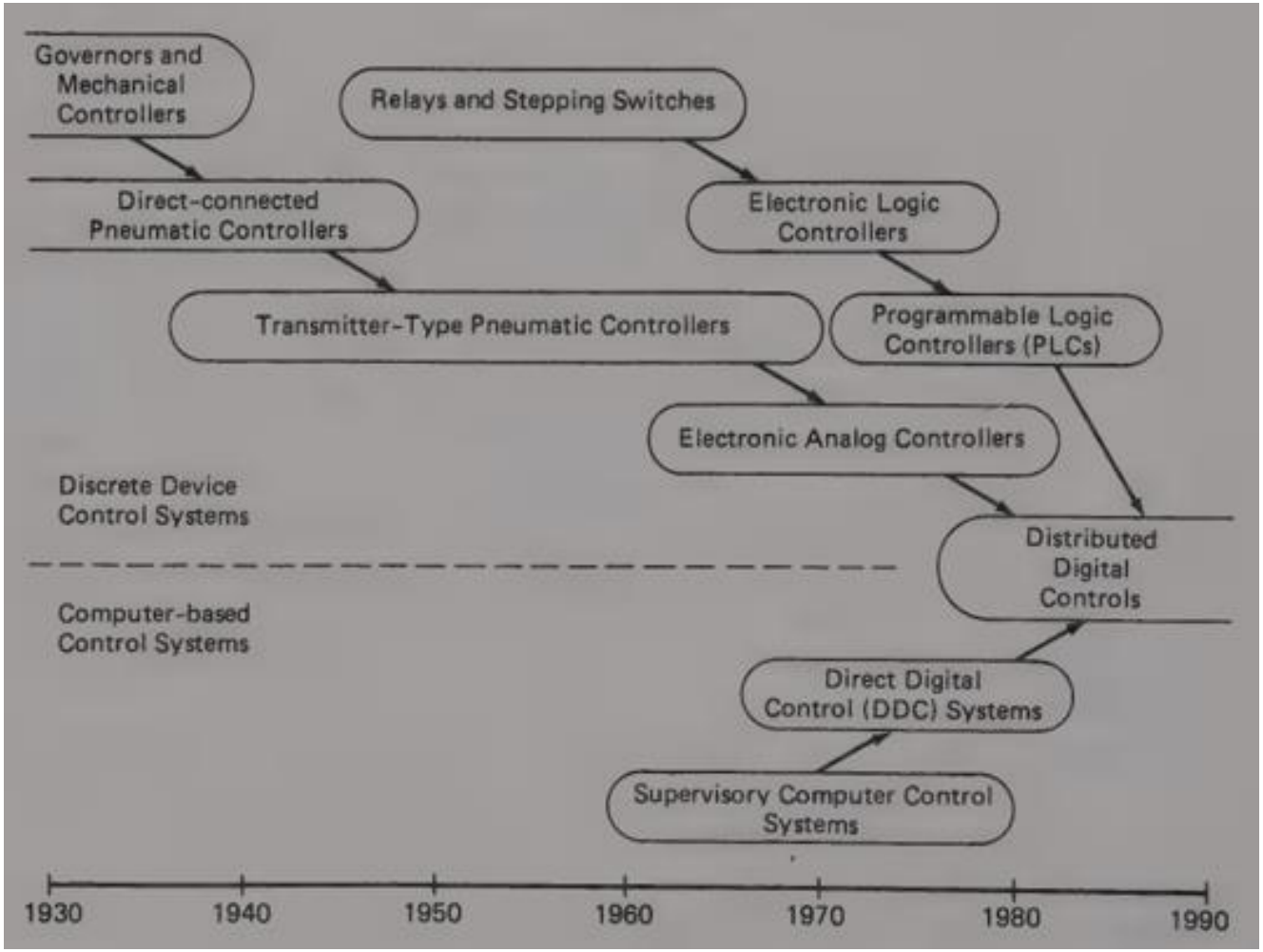
- Use of smart devices and field buses makes **DCS** to be prominent in large and complex industrial processes as compared to the former centralized control system.
- This distribution of control system architecture around the plant has led to produce more efficient ways to improve reliability of control, process quality and plant efficiency.

Control rooms then and now

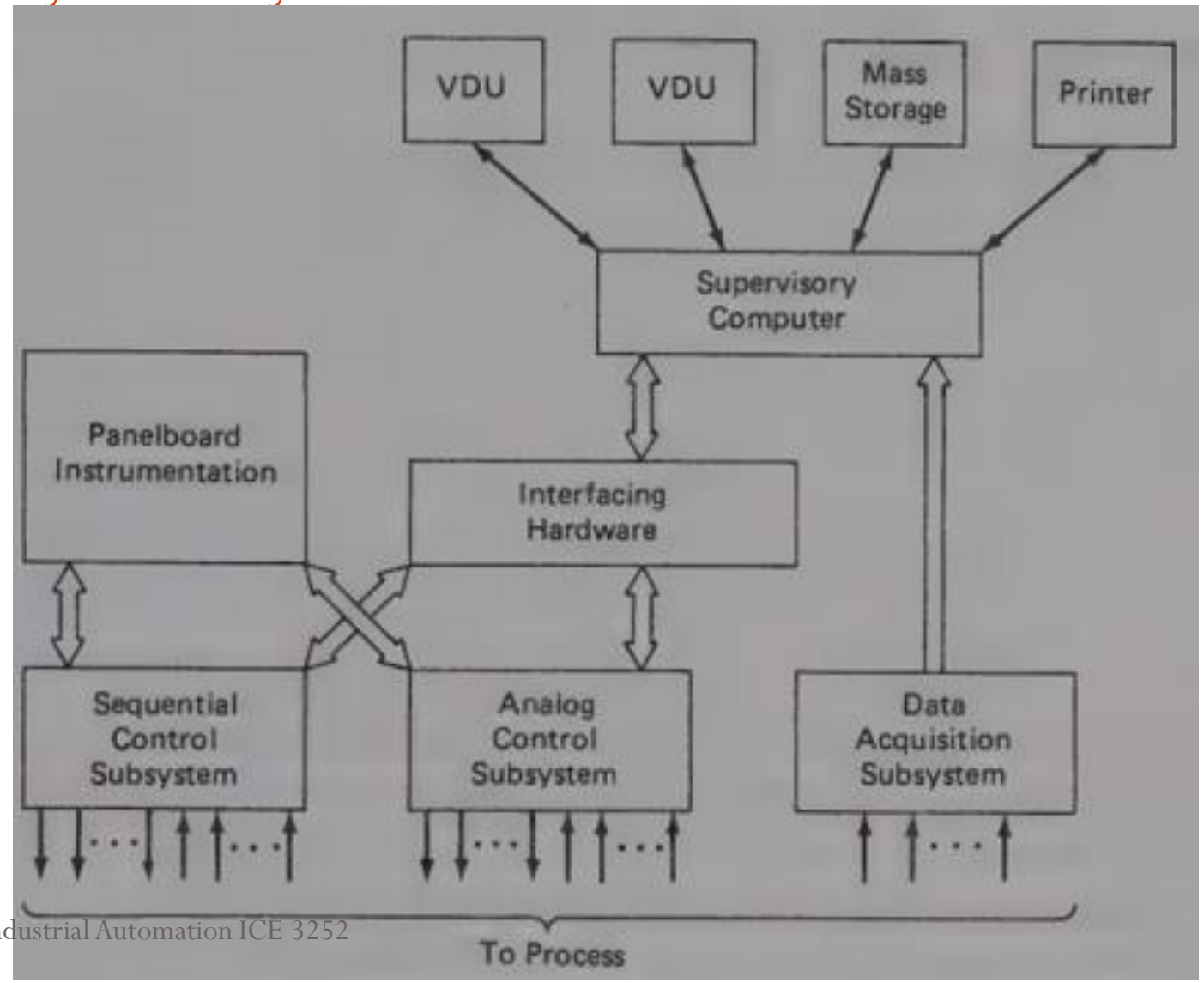
A pre-DCS era central control room. Whilst the controls are centralised in one place, they are still discrete and not integrated into one system.

A DCS control room where plant information and controls are displayed on computer graphics screens. The operators are seated as they can view and control any part of the process from their screens, whilst retaining a plant overview.

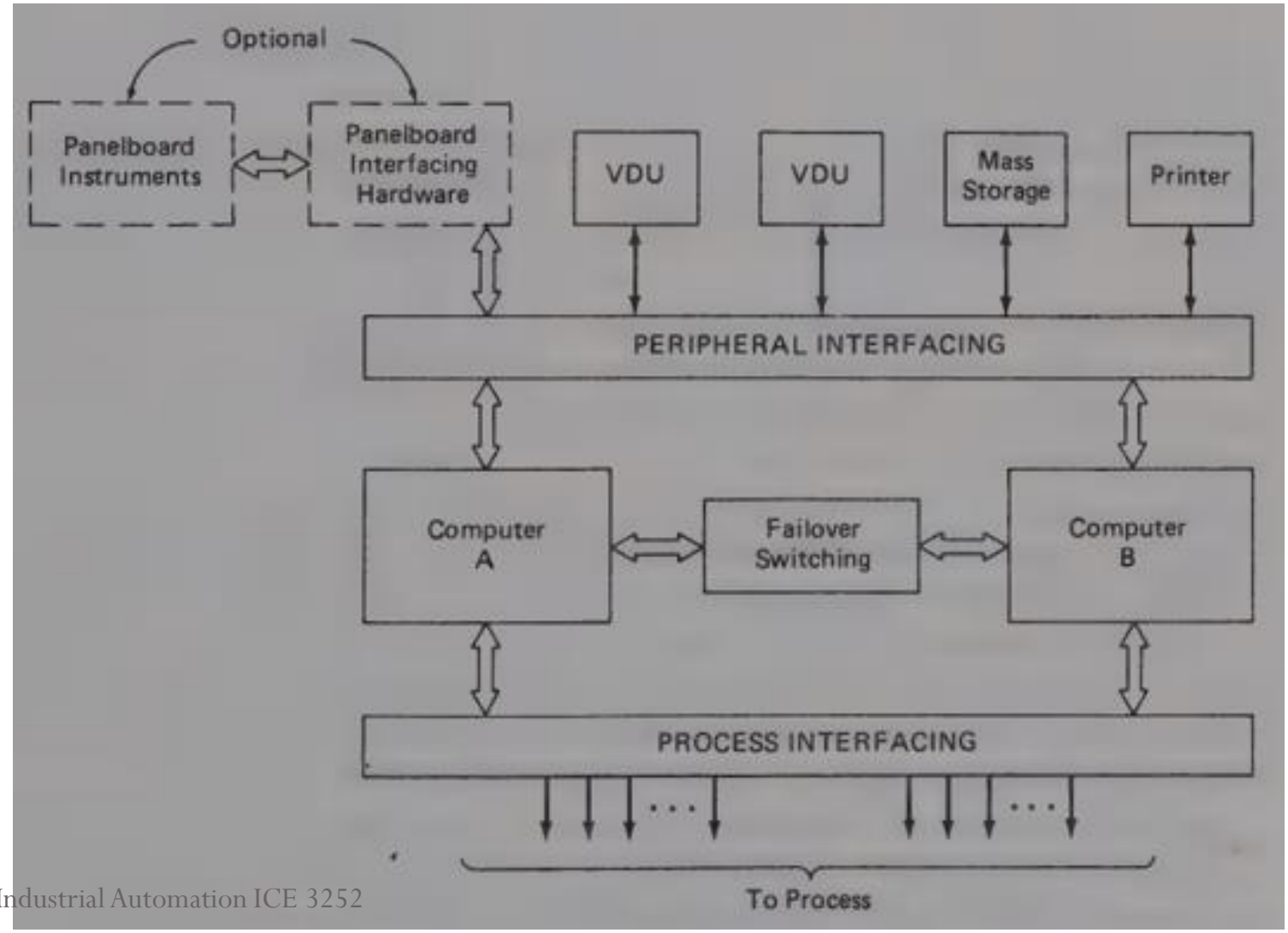
Evolution of industrial control technology



Hybrid system architecture



Centralized computer control system



Definition of DCS:

- A ***distributed control system*** is a specially designed computerised, automated control system that consists of geographically distributed control elements over the plant or control area, with many control loops.
- It differs from the centralized control system wherein a single controller at central location handles the control function, but in DCS each process element or machine or group of machines is controlled by a dedicated controller.
- DCS consists of a large number of local controllers in various sections of plant control area and are connected via a high speed communication network.

DCS

- DCSs available today can perform very advanced control functions, along with powerful recording, totalizing, mathematical calculations, and decision-making functions.

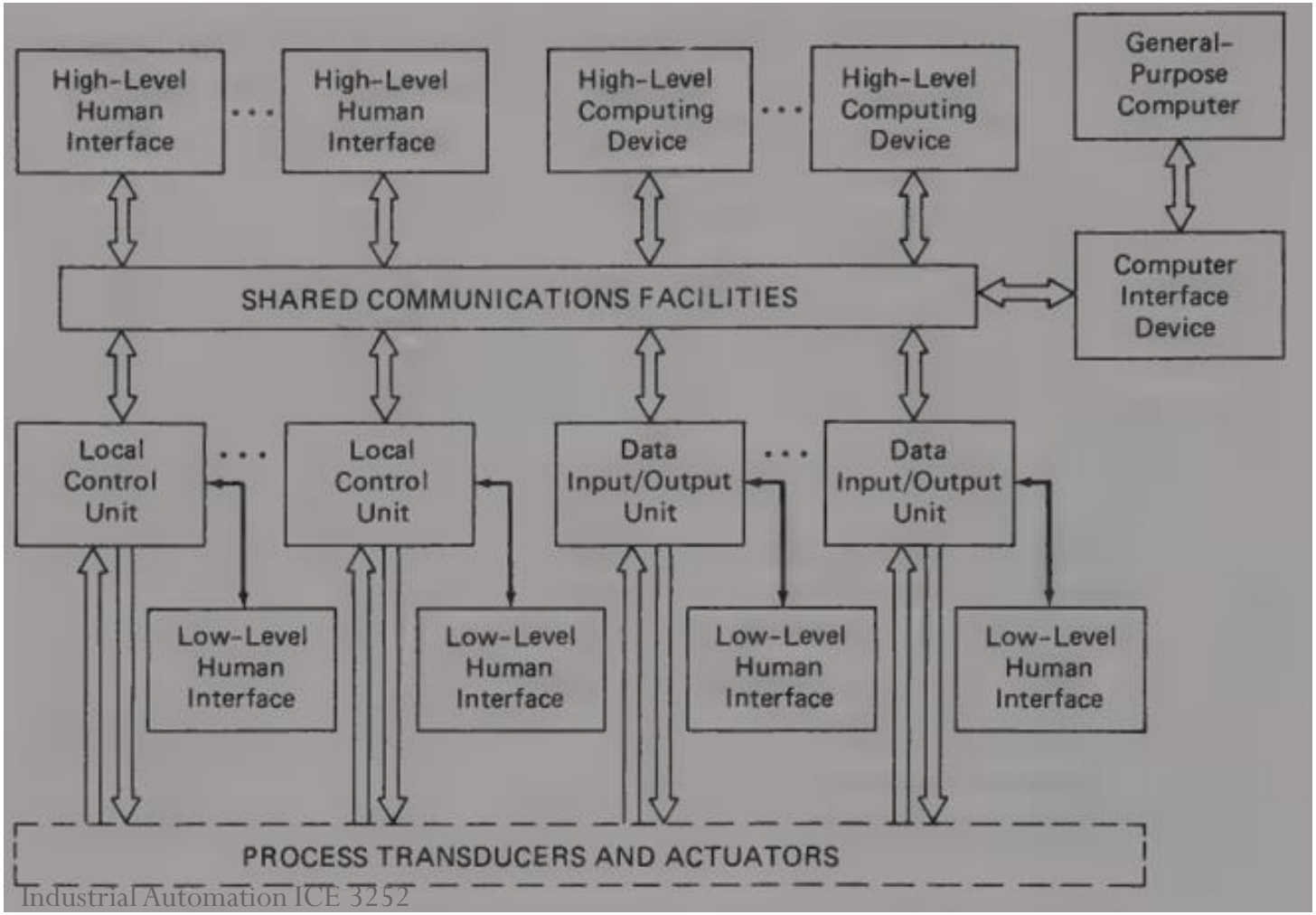
- In DCS control system, data acquisition and control functions are carried through a number of DCS controllers which are microprocessor based units distributed functionally and geographically over the plant and are situated near area where control or data gathering functions being performed.

- Distributed individual automatic controllers are connected to field devices such as sensors and actuators.

DCS

- These controllers ensure the sharing of gathered data to other hierarchal controllers via different field buses.
- Different field buses or standard communication protocols are used for establishing the communication between the controllers. Some of these include Profibus, HART, arc net, Modbus, etc.
- The main advantage of dividing control tasks for distributed controllers is that if any part of DCS fails, the plant can continue to operate irrespective of failed section.
- DCS first emerged in large, high value, safety critical process industries where manufacturer would supply both local control level and central supervisory equipment.

Generalized DCS



DCS elements

- Local control unit (LCU)
- Low level human interface (LLHI)
  - Low level operator interface
  - Low level engineering interface
- Data input/output unit (DI/OU)
- High level human interface (HLHI)
  - High level operator interface
  - High level engineering interface
- High level computing device (HLCD)
- Computer interface device (CID)
- Shared communication facilities

Comparison of architectures

FEATURE	HYBRID ARCHITECTURE	CENTRAL COMPUTER ARCHITECTURE	DISTRIBUTED ARCHITECTURE
1. Scalability and expandability	Good due to modularity	Poor—very limited range of system size	Good due to modularity
2. Control capability	Limited by analog and sequential control hardware	Full digital control capability	Full digital control capability
3. Operator interfacing capability	Limited by panelboard instrumentation	Digital hardware provides significant improvement for large systems	Digital hardware provides improvement for full range of system sizes
4. Integration of system functions	Poor due to variety of products	All functions performed by central computer	Functions integrated in a family of products
5. Significance of single-point failure	Low due to modularity	High	Low due to modularity
6. Installation costs	High due to discrete wiring and large volume of equipment	Medium—saves control room and equipment room space but uses discrete wiring	Low—savings in both wiring costs and equipment space
7. Maintainability	Poor—many module types, few diagnostics	Medium—requires highly trained computer maintenance personnel	Excellent—automatic diagnostics and module replacement

PLC vs DCS

- **Response time**
  - PLCs are fast, no doubt about it. Response times of one-tenth of a second make the PLC an ideal controller for near real-time actions such as a safety shutdown or firing control.
  - A DCS takes much longer to process data, so it's not the right solution when response times are critical. In fact, safety systems require a separate controller.
- **Scalability**
  - A PLC can only handle a few thousand I/O points or less. It's just not as scalable as a DCS, which can handle many thousands of I/O points and more easily accommodate new equipment, process enhancements and data integration.
  - If you require advanced process control, and have a large facility or a process that's spread out over a wide geographic area with thousands of I/O points, a DCS makes more sense.

PLC vs DCS

- **Redundancy**
  - Another problem with PLCs is redundancy. If you need power or fault tolerant I/O, don't try to force those requirements into a PLC-based control system. You'll just end up raising the costs to equal or exceed those of a DCS.
- **Complexity**
  - The complex nature of many continuous production processes, such as oil and gas, water treatment and chemical processing, continue to require the advanced process control capabilities of the DCS.
  - Others, such as pulp and paper, are trending toward PLC-based control.
- **Frequent process changes**
  - PLCs are best applied to a dedicated process that doesn't change often. If your process is complex and requires frequent adjustments or must aggregate and analyze a large amount of data, a DCS is typically the better solution.
  - Of course, the very flexibility of a DCS system also makes it much more vulnerable to "meddling/interference" by operators that can cause spurious shutdowns.

PLC vs DCS

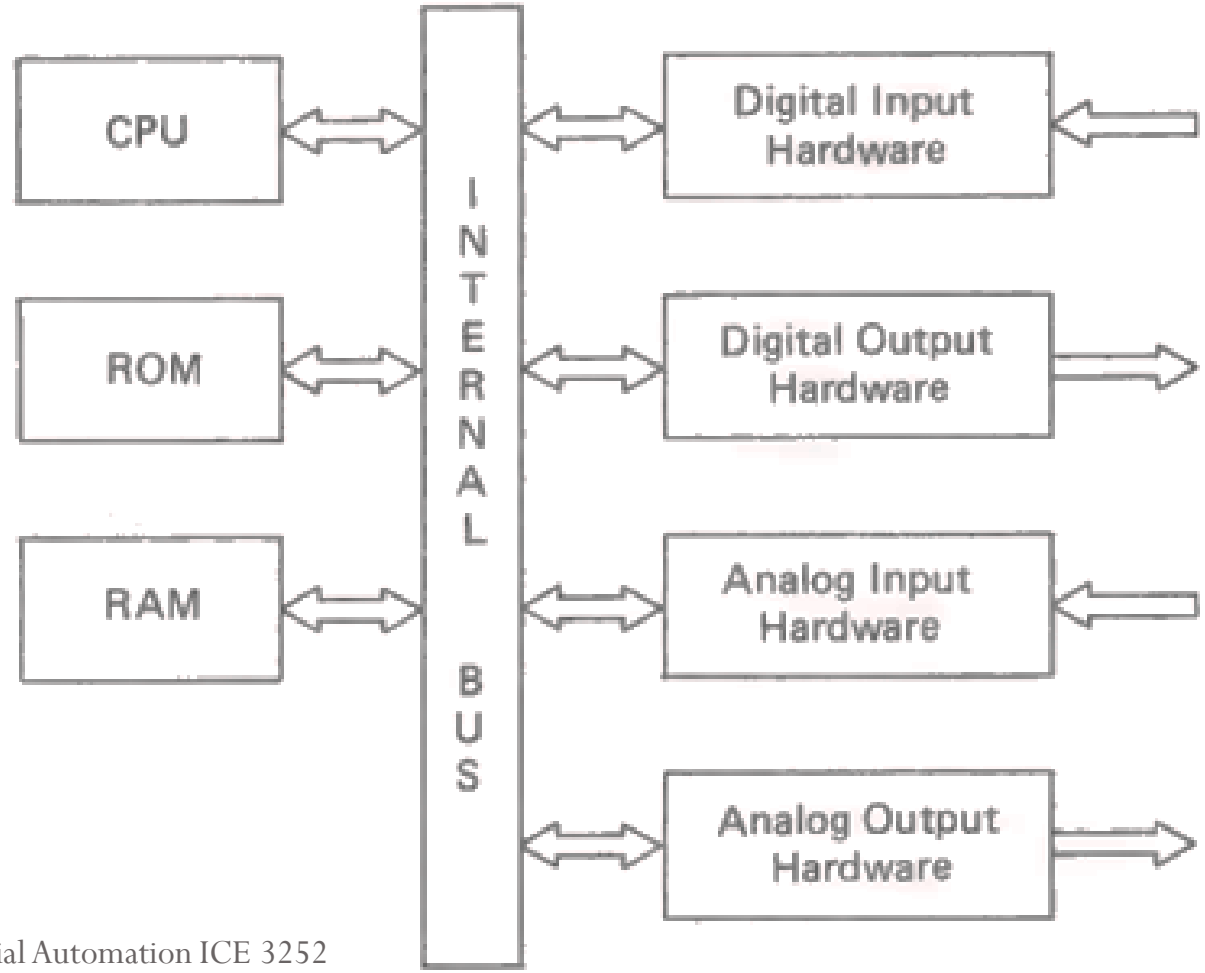
- **Vendor support**
  - DCS vendors typically require users to employ them to provide integration services and implement process changes.
  - System integrators perform similar functions for PLC-based systems. It has also become common for PLC vendors to offer support services through their network of system integrator partners.
  - Process control has become increasing complex. It's difficult for any individual to know everything about these sophisticated systems, increasing the need for vendor support.

Local Control unit

- LCU is the smallest collection of hardware in the distributed control system that performs closed loop control.

- Malfunctioning of LCU can cause a condition that is hazardous to both people and equipment, its proper design is critical to the safe and efficient operation of the plant.

Basic elements of LCU



LCU architecture requirements

- Flexibility of changing the control configuration
- Ability to use the controller without being a computer expert-should allow the user to configure the LCU control algorithm in a simple way
- Ability to bypass the controller in case it fails so that the process still can be controlled manually.
- Ability of the LCU to communicate with other LCUs and other elements in the system

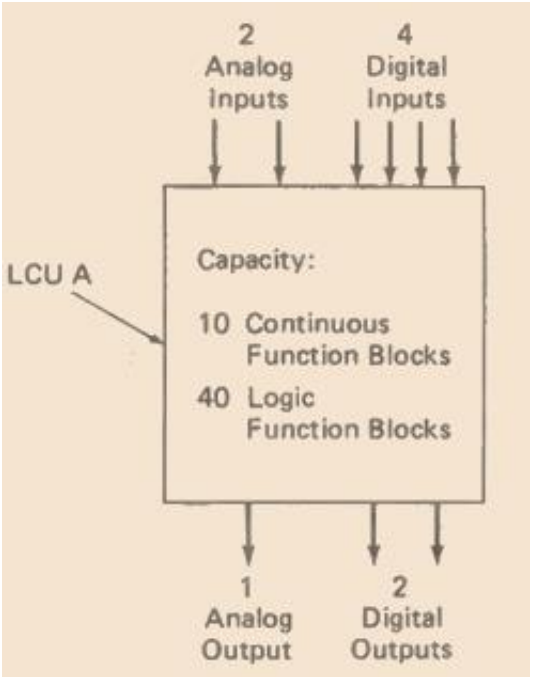
LCU architectures

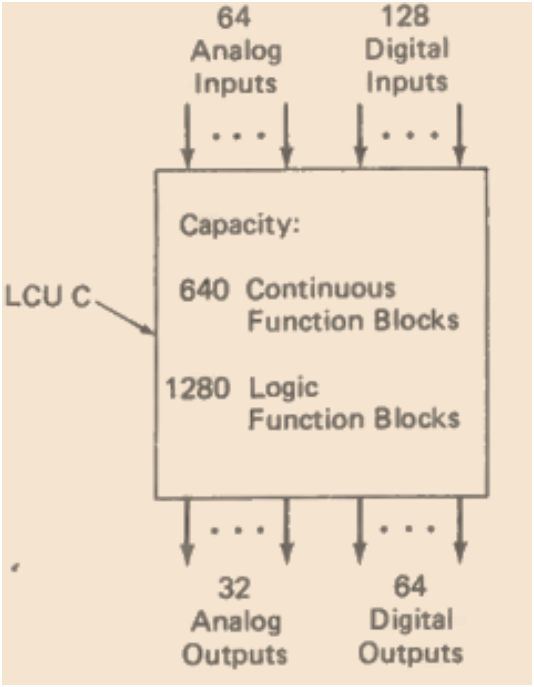
Architectural parameters

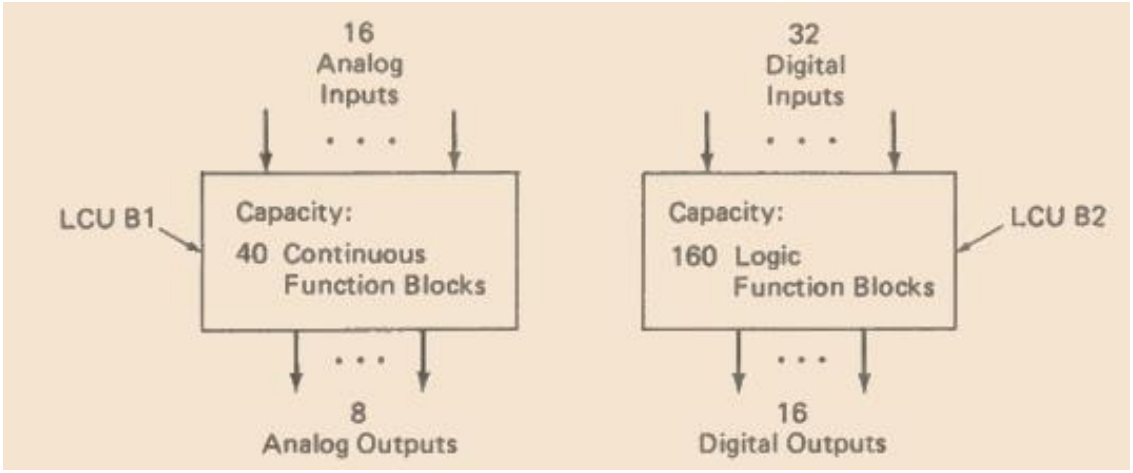
- Size of controller-represents the number of functional blocks and/or language statements that can be executed and no. of I/O channels provided by the controller.
- Functionality of controller- refers to the mix of functionality blocks or language statements provided by the controller(e.g. continuous control, logic control, arithmetic functions or combination of these).and process input output types (analog or digital)
- Performance of controller-refers to the rate at which the controller scans inputs, function blocks or statements and also refers to the accuracy with which the controller performs these operations.
- Communication channels out of controller-the number, type and speed of the communication channels to operator interface devices and other controllers and devices in the system.
- Controller output security-refers to the provision of manual or backup redundancy to ensure that the control output is maintained despite of controller failure

LCU architecture configurations

- Configuration A
- Configuration B
- Configuration C







Comparison of architectures

ARCHITECTURE PARAMETERS	CONFIGURATION A (SINGLE-LOOP)	CONFIGURATION B (2 LCU TYPES)	CONFIGURATION C (MULTI-LOOP)
Controller size	Number of functions needed for single PID loop or motor controller.	Includes functions and I/O needed for eight control loops and a small logic controller.	System size is equivalent to small DDC system.
Controller functionality	Uses both continuous and logic function blocks.	Continuous and logic function blocks split between controllers.	Uses both continuous and logic function blocks; can support high-level languages.
Controller scalability	High degree of scalability from small to large systems	Requires both controller types even in small systems.	Not scalable to very small systems.
Controller performance	Requirements can be met with inexpensive hardware.	Because of functional split, performance requirements are not excessive.	Hardware must be high performance to execute large number of functions.
Communication channels	Need intermodule communications for control; only minimum needed for human interface.	Functional separation requires close interface between controller types.	Large communication requirement to human interface; minimal between controllers.
Controller output security	Controller has single-loop integrity; usually only manual backup is needed.	Lack of single-loop integrity requires redundancy in critical applications.	Size of controller requires redundancy in all applications.

LCU Languages

Language must allow the user to implement at least the set of control functions that have been provided in the past by conventional analog, sequential, and Programmable control systems. Communication functions also are required to allow the LCUs to exchange information with other elements in the distributed control system. A representative list of these control and communication functions includes:

- Data acquisition and signal conditioning functions, such as input scanning, filtering, linearization, and conversion to engineering units;
- Limit checking and alarming functions;
- Modulating control functions, including PID control with all its variations;
- Sequential control functions for implementing Boolean logic
- Computational functions, such as arithmetic, trigonometric, and dynamic signal processing (integral, derivative. and filter) functions;
- Signal output functions, both for control and for driving recorders and indicators;
- Communication functions to allow signal transmissions between.th LCU and other controllers and elements in the distributed control system;
- Communication functions to human interface devices that allow operators and engineers to interact with the LCU.

LCU languages

- As the user of DCS is not likely fluent in machine level language in terms of bits and bytes, a high level language must be provided to allow him to interact hardware.
- FORTAN and BASIC were the majorly used general purpose language in earlier DCS.
- The current major languages include-functional blocks, problem oriented languages

High level language features required in DCS

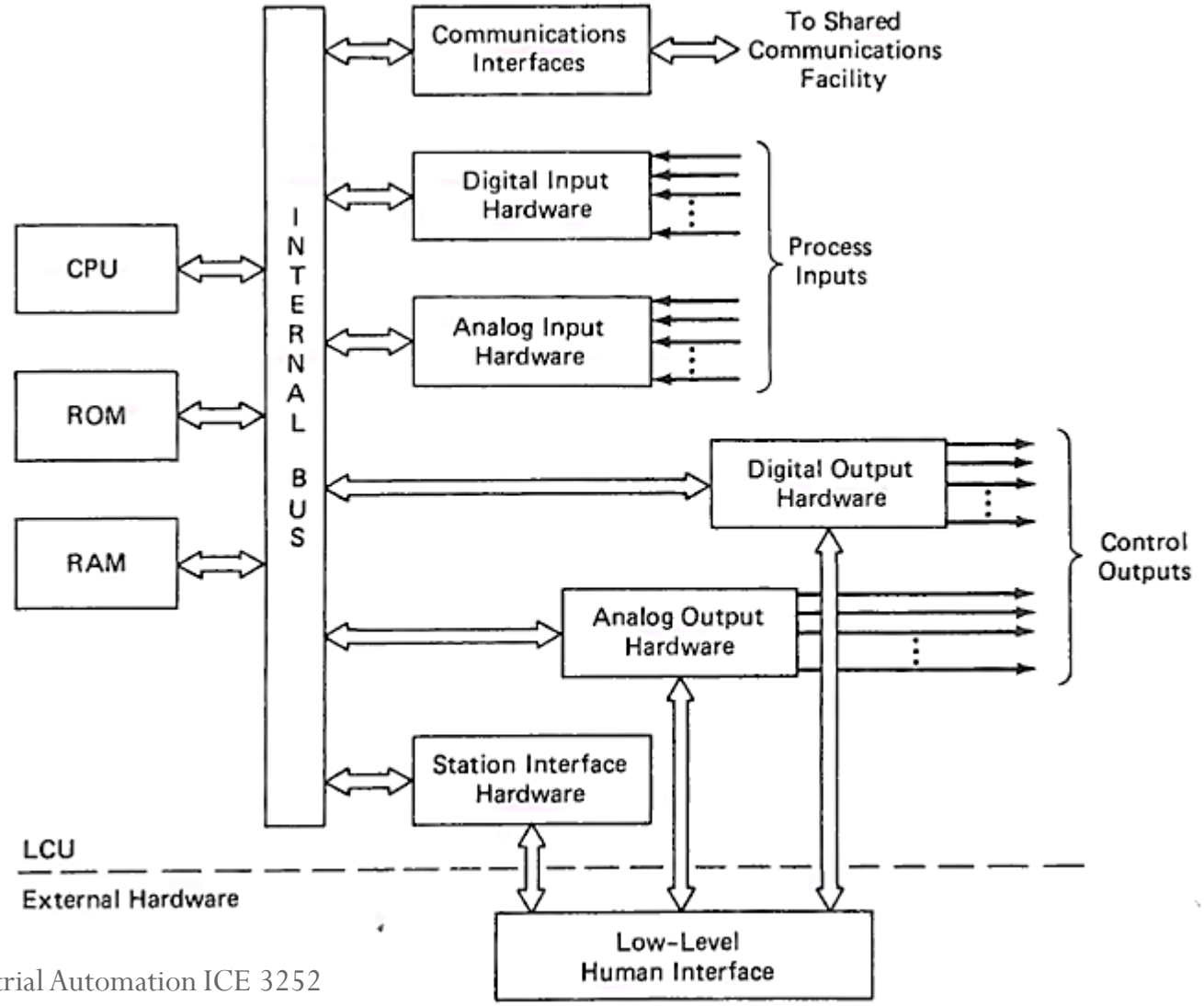
- interfacing with the process;
- coping with the real-time environment;
- interfacing with other elements in a distributed control system;
- providing the security features required in a control application;
- supporting the utilities required to write and maintain the programs.

LCU Process interfacing issues

The low-level human interface device and its associated interface hardware allow several important human interfacing functions to be accomplished through hardware that is connected directly to the LCU rather than over the shared communication facilities. These functions include:

- Allowing the plant operator to control the process (e.g., select control set points and controller modes)
- Allowing the operator to override the automatic equipment and control-the process manually in case of a controller hardware failure or other system malfunction
- Allowing the plant instrumentation engineer to configure the control system logic and later tune the control system parameters.

LCU interface to DCS



LCU process interfacing issues

- Security design issues for LCU
  - Security requirements
  - Security design approaches
  - On-line diagnostics
  - Secure control output designs
  - Manual backup deigns
  - Redundant controller designs
- Process I/O design issues
  - I/O requirements
  - I/O design approaches
  - Design of field terminators

Security design issues

- Security requirements
  - The first priority-Safe operating conditions
  - Downtime –decreases production which is extremely expensive, an unsafe condition that leads to human injury or plant damage is still expensive. Hence reliability is one of the major factors considered in evaluating a DCS.
  - Thus by use of highest quality components, conducting expensive testing of the hardware and implementing other quality control measures, a highly reliable control system can be manufactured.

Security objectives necessary in designing a DCS

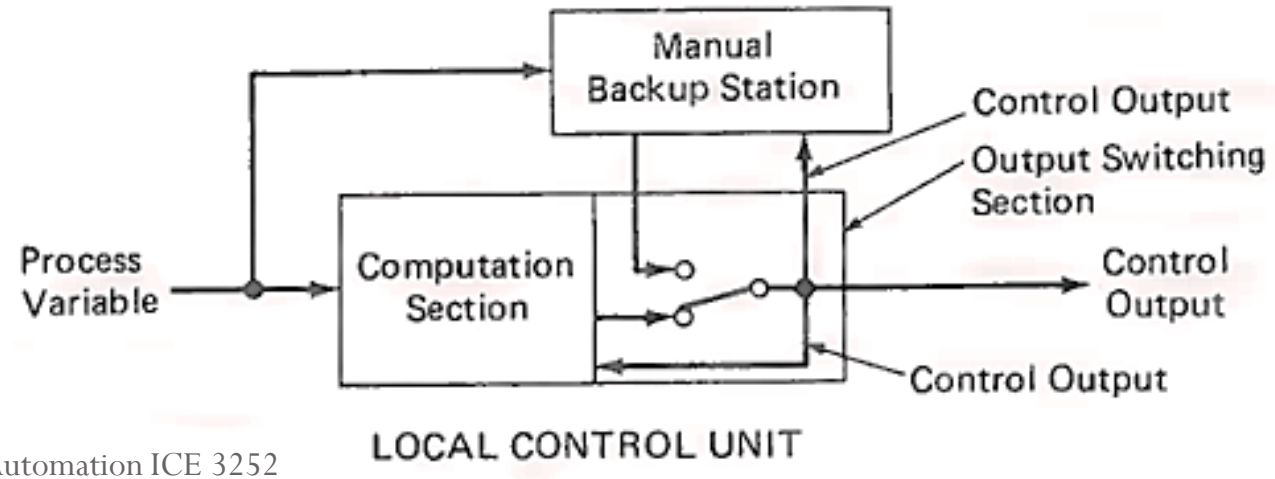
- Maximize the availability of the automatic control functions of the system. As much as possible. make sure that the failure of a single control system element does not shut down all automatic control functions.
- If the failure of a control system element causes the loss of automatic control in a portion of the system. make sure that there is a mechanism that allows the operator to take over manual control of that portion.
- As much as possible. ensure that the control' outputs to the process are safe ones so that if critical automatic and manual control functions are lost. the operator can. shut the process down in an orderly and safe manner.

Security design approaches

- Provide manual backup only
- Provide a standby redundant controller
- Provide multiple active controllers

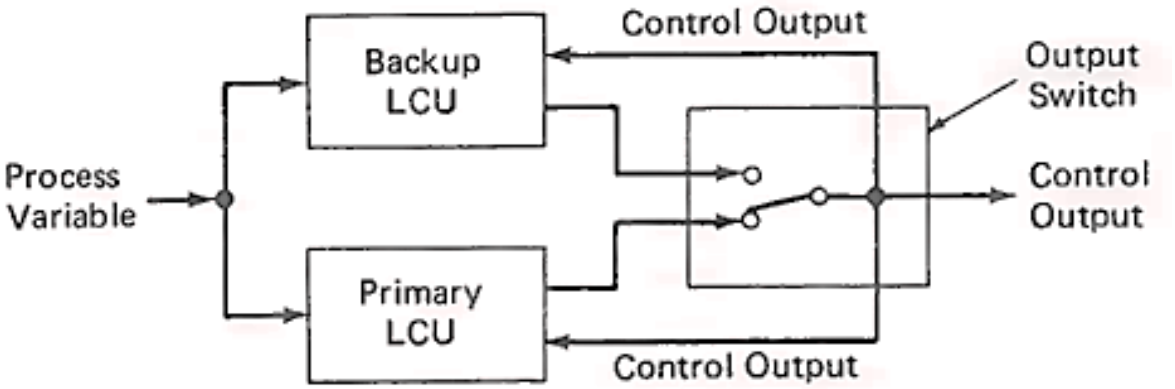
Manual backup approach

- In this case, each LCU is designed to implement only one or two control loops and reliance is placed on the operator to take over manual control in case of a failure of the LCU.
- The control output is fed back to the manual backup station and to the computation section of the controller so that the inactive element can synchronize its output with the active element.
- This ensures that the process will not be bumped when a switchover from the active to the inactive device occurs.



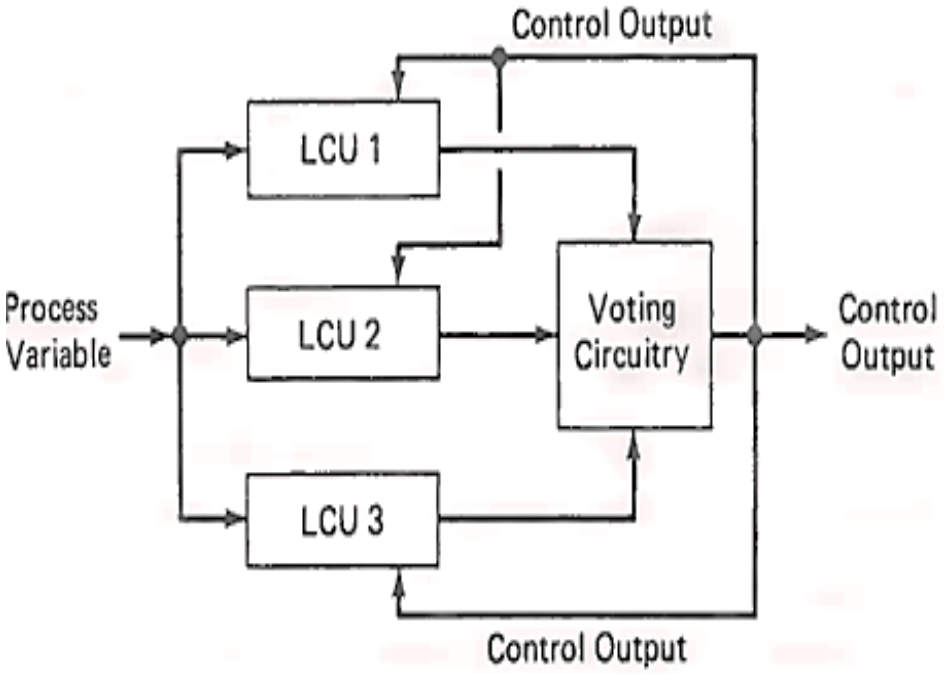
Hot standby redundancy approach

- The LCU is backed up by another LCU that takes over if-the primary controller fails.
- In this way, full automatic control is maintained under failure conditions.
- As in the first case control output is fed back to both controllers to allow bump less transfers to be accomplished.



Multiple active redundant controllers

- Several LCUs are active at the same time -in reading process inputs, calculating control algorithms, and producing-control outputs to-the process.
- Since only one output can be used at a time, voting circuitry selects the valid output.
- The multiple active approach is designed so that a failure of one of the controllers does not affect the automatic control function.
- The selected control output is fed back so that each controller can compare its own output with the output generated by the voting device.



Online diagnostics

- Once a diagnostic test has detected a failure, the LCU must be able to act on this information in one or more of the following ways:
- The LCU should be able to alarm or report the failure to both the low-level human interface and to the higher-level human interface and computing elements. If-possible, both the existence and the type of failure should be reported.
- The LCU should, be able to switch a contact output to provide an external hardware indication of failure.
- If the failure affects only a portion of the LCU, the internal application logic of the LCU should be able to drive a failure indicator.(e .g., manual instead of automatic, or simple loop instead of cascade.)
- The LCU should be able to shut itself down in an orderly way if necessary.

Secure control output design

- Keep the number of analog outputs per D/A converter to a minimum.
- Design both analog and digital output circuitry so that the Control outputs go to a safe state when the LCU fails
- If possible, power the output circuitry from a supply that is independent of the supply used to power the rest of the LCU. The safe output states can then be generated even if the rest of the LCU is not operating either from loss of power or other failure conditions
- Design the output circuitry so that the actual value of the output can be read back by the rest of the LCU. This feature provides two benefits: it permits the LCU to verify that the correct control output has been generated and it allows the transfer between the LCU and manual backup stations or redundant controllers to be bumpless.
- For maximum reliability of each output channel, minimize the number of components and electrical connections between the control output driver hardware and the field termination point for the control actuator.

Manual backup designs

- The first step of defense against failure in the control system is to include the output security features discussed in the LCU design.
- The next step of defense providing a manual backup capability to allow the operator to take direct control over the outputs affected by a control system failure. This is usually accomplished through a low-level operator interface that is directly connected to the LCU.
- Proper design of the manual backup circuitry is extremely important to control system security.

Redundant controller designs

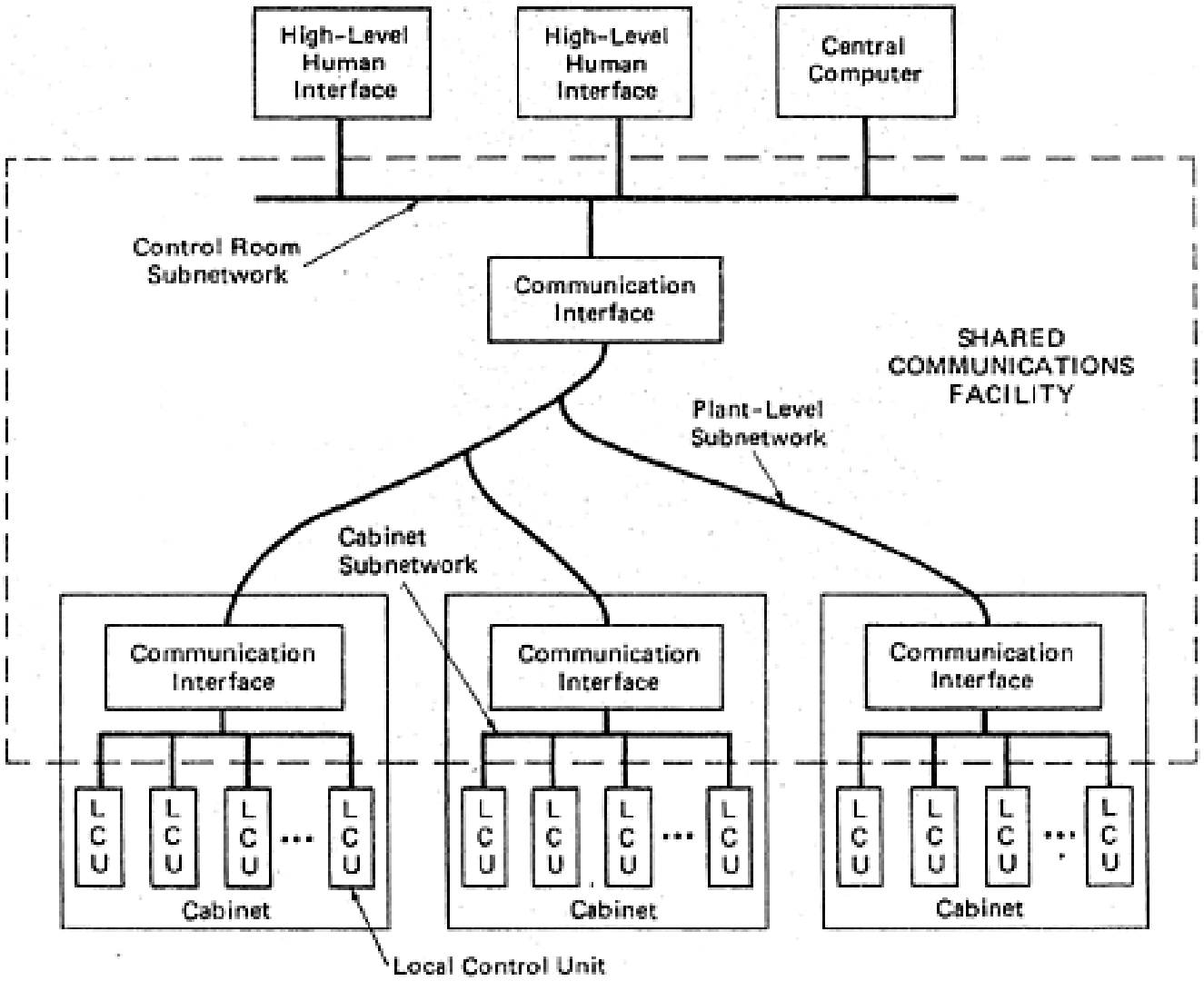
By default the redundant control system structure are more complex than those that rely on manual backup. Thus some guidelines have to be followed while designing a redundant control system are:

- The redundant architecture should be as simple as possible.
- The architecture must minimize potential single points of failure
- The redundant nature of controller configuration should be transparent to the user.
- The process should not be disturbed or bumped when the one of the redundant elements fails
- The redundant LCU architecture must have the capability for hot spare replacement that is, allow for the replacement of failed redundant elements without shutting down the total LCU.

Process I/O design issues

- There are several dimensions to the problem of providing cost-effective I/O hardware for a distributed control system.
- The first dimension is simply the large variety of I/O signals that the control system must handle in order to interface with sensors, analysers transmitters, control actuators and other field-mounted equipment.
- The second dimension in providing cost effective I/O hardware is the wide range of I/O performance specifications that are imposed to facilitate interfacing with various types of field equipment.
- The third dimension is the varying degree of I/O hardening required in different applications.

DCS communication architecture



Communication System Partitioning

Operator interface

Two distinct groups of plant personnel interact with the control system on a regular basis.

- Instrumentation and control system engineers-These people are responsible for setting up the control system initially and adjusting, and maintaining it from time to time afterwards
- Plant operators-These people are responsible for monitoring, supervising, and running the process through the control system during startup, operation, and shutdown conditions.

The human interface is provided through

1. Through a low-level human interface (LLHl) connected directly to the local control unit or data input/output unit (Dl/OU) via dedicated cabling
2. Through a high-level human interface (HLHI) connected to an LCU or DI/OU only through the shared communications facility.

Low level operator interface [LLOI]

There are a number of motivations for using an LLOI:

- It provides an interface that is familiar to operators trained to use panel board instrumentation, since it is usually designed to resemble that type of instrumentation;
- It is usually less expensive than HLOI in small applications say, less than 50 control loops)
- It can provide manual backup in, case the automatic control equipment or the HLOI fails.
- LLOI hardware resembles panel board instrumentation.

High level operator interface [HLOI]

- HLOI in a distributed control system is a shared interface that is not dedicated to any particular LCU. Rather, the HLOl Is used to monitor and control the operation of the process through any or all of the LCUs in the distributed system.
- HLOI hardware uses CRT or similar advanced display technology in console configuration often referred as VDU.
- The HLOI accepts operator inputs through keyboards instead of the switches, push-buttons, and potentiometers- characteristic of conventional operator interface panels.
- Microprocessor-based digital technology is used in the design of the HLOI system providing the benefit like:
  - Significant reduction in control room space
  - Improved flexibility in creating operator interface
  - Permits cost effective implementation of functions that previously could be accomplished only with expensive computers.

Low level engineering interface [LLEI]

- It is a microprocessor based device designed as an electronic module that mounts in a rack or as hand held portable device.
- To minimize cost. the device usually is designed with a minimal keyboard and alphanumeric display so that the instrument engineer can read data from and enter data into the device.
- Some versions of LLEI must directly connect to one local unit or DI/OU at a time. More sophisticated version can connect to a local branch of the shared communications facility and are able to communicate with any one of several LCUs or DI/OU in adjacent areas of the plant.
- The LLEI can be connected or disconnected while the LCU or DI/OU is powered and on operation, it is not necessary to shut the process down.

High level engineering interface[HLEI]

- The HLEI allows a-user to reap the full benefits of the flexibility and control capabilities of a distributed control system while minimizing the system engineering costs associated with such a system.
- More expensive than LLEI but is extremely cost effective when used in conjunction with medium to large scale systems.
- The HLEI is implemented in the form of a CRT-based console, or V'DU, similar to the high-level operator interface unit.

Reference

- Lukcas M.P, *Distributed Control Systems*, Van Nostrand Reinhold Co., 2016.