PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
UNIVERSITY YAHIA FARES OF MEDEA
Faculty of Technology
Department of Process and Environmental Engineering

SAFETY OF INDUSTRIAL INSTALLATIONS AND EQUIPMENT

Complete course — lecture notes, tutorials and appendices

Bachelor (Licence) L3 — Industrial Hygiene and Safety
Semester 5 · Teaching unit UEF 3.1.2 · 67 h 30 · 6 credits · coefficient 3
Language of instruction: English

Dr. Ahmed Cherif RAHMANI
Maître de conférences classe B
rahmani.ahmedcherif@univ-medea.dz · ORCID 0009-0008-9766-4933

Academic year 2026–2027

Table of contents

Course presentation

Aim of the course

The official programme states the aim in one sentence: to diagnose hazardous situations in installations and during the use of machinery, to define safety zones, and to understand how machines function and how they are used. This book develops that aim into a working method rather than a body of facts to be memorised.

The method is the one on which the whole international body of machinery safety standards rests. Identify the hazards. Estimate and evaluate the risk. Then reduce it in a fixed order of priority — first by design, then by safeguarding and complementary protective measures, and only last by information for use. A student who leaves this course able to apply that sequence to an unfamiliar machine, and to justify each choice against a named standard, has met its objective.

Learning outcomes

On completion of the course you are able to:

- situate a machine or installation within the applicable legal and normative framework, and distinguish what the law requires from what a standard recommends;
- use the vocabulary of ISO 12100 correctly — in particular hazard, hazardous situation, hazardous event, harm and risk, which are not synonyms;
- conduct a structured risk assessment on a machine, document it, and rank the resulting risks;
- apply the three-step method of risk reduction in the correct order, and justify why a given measure was selected;
- calculate a safety distance and position a safeguard, stating the assumptions used;
- select an appropriate guard or protective device, and state its limits;
- read a safety-related control architecture, identify its safety function, and explain what Performance Level and Safety Integrity Level express;
- describe the safety life cycle of a safety instrumented system and the role of proof testing.

Structure and time allocation

Weeks	Chapter	Object
1–2	Chapter 1	Where safety requirements come from, and who is bound by them
3–4	Chapter 2	The vocabulary without which no assessment is possible
5–7	Chapter 3	From the machine to the installation and its neighbours
8–11	Chapter 4	The technical core: keeping the person out, or stopping the machine in time
12–15	Chapter 5	When safety itself depends on a system that can fail

Assessment

Continuous assessment counts for 40 % and the final examination for 60 %.

Component	Weight	Form and timing
Graded tutorial submissions	15 %	Three submissions, weeks 4, 9 and 13, individual, in PDF
Chapter tests	15 %	Two graded quizzes, weeks 7 and 14, time-limited, one attempt
Machine risk assessment report	10 %	One short report on a real machine, in pairs, week 12
Final examination	60 %	Written, covering the five chapters

How to use this book

Each chapter is self-sufficient and can be read without having attended the lecture. Every chapter ends with a summary in bullet points and six self-check questions. The summary is the revision trame; the questions are the test of whether you have understood, and several of them reappear, in another form, in the examination.

Passages set off by a vertical rule in the margin are practical remarks: the frequent error, the point of vigilance, the question to expect. They are not decorative, and they are examinable.

> *One habit to acquire from the first week. Whenever you meet a requirement — in this book, in a plant, in a supplier document — ask three questions: is it a legal obligation or a technical recommendation, whom does it bind, and what happens if it is not met. If you cannot answer the three, you have not understood the requirement.*

UNIVERSITY YAHIA FARES OF MEDEA · FACULTY OF TECHNOLOGY
Department of Process and Environmental Engineering

Chapter 1 — The Normative Framework

Safety of Industrial Installations and Equipment · L3 Industrial Hygiene and Safety

Weeks 1 and 2 · Lecture notes · Dr. A. C. Rahmani

What this chapter is for

Before studying any technical measure, one has to know where the requirement comes from and who is bound by it. This is not a formality. A guard that satisfies the law may not satisfy the standard; a machine that complies with the standard may still be used unsafely by an employer who has other obligations altogether. Confusing these two orders of requirement is the most common error made by young safety engineers, and it has a cost: measures are taken that no one asked for, while obligations that do exist are left unmet.

At the end of this chapter you should be able to say, for any requirement placed before you, whether it is a legal obligation or a technical recommendation, whom it binds, and what happens if it is not met.

1.1 Two distinct orders: law and standards

A law or a regulation is adopted by a public authority and is binding. It states an obligation of result — the machine must not endanger the operator — and it provides a sanction. It rarely says how the obligation is to be met, because a legal text that prescribed a technique would become obsolete with that technique.

A standard is a technical document produced by a standards body, in which manufacturers, users, laboratories and administrations sit together. It states the state of the art at the moment it was written. In principle a standard is voluntary: nothing compels a manufacturer to apply it. In practice its authority is considerable, for two reasons that must be understood separately.

The first is legal. Where a legal framework provides for it, applying a standard that has been recognised for that purpose confers a presumption of conformity: the manufacturer who applied it is presumed to have met the corresponding legal requirement, and it is then for the authority to prove otherwise rather than for the manufacturer to prove compliance. This is the mechanism used in the European Union under the harmonised standards system, and it is worth understanding even outside Europe, because it explains why manufacturers follow standards they are not obliged to follow.

The second is evidential. In the event of an accident and of litigation, the standard is the reference against which the behaviour of the manufacturer or of the employer will be measured. Departing from it is possible, but the burden of demonstrating an equivalent level of safety then falls on the one who departed.

> *Keep this distinction in mind throughout the course: the law says what must be achieved, the standard says how it is usually achieved. Neither replaces the other, and neither is optional in practice.*

1.2 The Algerian framework

In Algeria the general obligation rests on Law no. 88-07 of 26 January 1988 on occupational health, safety and medicine. It establishes that the employer is responsible for the health and safety of workers, that work equipment must be maintained in a condition that does not endanger them, and that the organisation of work must take safety into account. Implementing texts specify particular sectors and particular equipment.

For installations that present a risk to the environment or to neighbouring populations, the framework of classified installations applies, under the environmental protection legislation. Such installations are subject to authorisation or declaration according to their category, and to a hazard study proportionate to the risk. This is the point of contact between the safety of a machine, which concerns the operator, and the safety of an installation, which may concern a whole district — a distinction taken up in Chapter 3.

Technical standards are adopted nationally by IANOR, the Algerian standards institute, which publishes Algerian standards under the prefix NA. A large part of the machinery safety corpus consists of international standards adopted as such. In practice, therefore, the technical content of this course is the international content, and the reference numbers you will meet in industry are those of ISO and IEC.

1.3 The European system, and why it is studied here

Two reasons justify studying the European system in an Algerian course. Much of the machinery installed in Algerian industry is designed for the European market and arrives with European conformity documentation; and the international standards that Algeria adopts were, for the most part, developed under that system and carry its logic.

The new approach

The European legislator sets out essential health and safety requirements in a legal text, and leaves the technical translation to standards bodies. The legal text says that machinery must be designed so that persons are not exposed to hazards when it is used as intended; the standard says how far a guard must be placed from a rotating part. The manufacturer who applies the relevant harmonised standard benefits from the presumption of conformity described above.

From directive to regulation

Machinery placed on the European market has been governed since 2006 by the Machinery Directive 2006/42/EC. That text is being replaced. Regulation (EU) 2023/1230 was adopted on 14 June 2023, entered into force on 19 July 2023, and applies from 20 January 2027 — the same date on which the Machinery Directive is repealed. There is no overlapping transition period.

The change of legal instrument matters. A directive must be transposed into the national law of each member state, which produces twenty-seven national texts and as many possible interpretations. A regulation applies directly and identically everywhere. The substantive changes are also real: the new text treats software, connected machinery and cybersecurity within the risk assessment, and revises the categories of machinery for which the involvement of an independent body is compulsory.

> *You will meet machines bearing conformity documents drawn up under the Directive and, from 2027, machines bearing documents drawn up under the Regulation. Both will be in service side by side for decades. Being able to read the two is part of the job.*

1.4 The three types of standard

Machinery safety standards are organised in three levels. Knowing which type you are holding tells you immediately what to expect from it.

Type	What it contains	Examples
Type A — basic safety standards	Basic concepts, principles of design and general aspects applicable to all machinery. There is essentially one of them.	ISO 12100 — general principles for design, risk assessment and risk reduction
Type B — generic safety standards	One safety aspect (B1) or one safeguard (B2), applicable across a wide range of machinery.	B1: ISO 13857 safety distances; ISO 13855 positioning of safeguards; ISO 13849-1 and IEC 62061 control systems. B2: ISO 14120 guards; ISO 14119 interlocking devices; ISO 13850 emergency stop
Type C — machine safety standards	Detailed requirements for one particular machine or family of machines. Where a type C standard departs from a type A or B standard, the type C standard prevails.	Standards for presses, for woodworking machines, for industrial robots, for agricultural machinery

The practical rule follows from the last line of the table. Look first for a type C standard covering your machine. If one exists, it is your primary reference. If none exists — and for a great many machines none does — you build your assessment on ISO 12100 and draw the specific requirements from the relevant type B standards.

1.5 ISO 12100 and the logic of the whole corpus

ISO 12100 is the standard from which the rest of the course descends. It is worth stating its logic now, in outline, because every subsequent chapter is an application of it.

It prescribes an iterative process. Determine the limits of the machine — what it does, who uses it, over what life, in what space. Identify the hazards, at every stage of the machine life including maintenance, setting and cleaning, which is where a large share of accidents occurs. Estimate the risk for each hazard, from the severity of the possible harm and the probability of its occurrence. Evaluate whether risk reduction is required. If it is, reduce it, and then begin again, because a protective measure may generate a hazard of its own.

The three-step method

Risk reduction follows a strict order of priority. The order is not a preference; it is a requirement, and inverting it is the classic fault in an examination answer.

Step	Measure	Illustration
1	Inherently safe design: eliminate the hazard or reduce the risk by design, before any guard is considered	Remove a pinch point by changing the geometry; reduce the force or the speed; use a non-flammable fluid; place the drive where no one has to reach across it
2	Safeguarding and complementary protective measures: where the hazard cannot be designed out, prevent access to it or stop the machine when access occurs	A fixed guard; an interlocked movable guard; a light curtain; an emergency stop device
3	Information for use: warn about the residual risk that remains after steps 1 and 2	Signs on the machine; instructions in the manual; required training; prescribed personal protective equipment

> *Why the order is binding: a warning sign placed where a design change was possible transfers the risk from the manufacturer to the operator. That is precisely what the standard forbids. A measure at step 3 is legitimate only for the risk that survives steps 1 and 2.*

1.6 Who owes what: manufacturer and employer

Two distinct sets of obligations apply to the same machine, at two different moments, and a safety engineer must be able to say which applies to him.

	The manufacturer	The employer or user
When	When the machine is designed and placed on the market	Throughout the working life of the machine, from installation to disposal
Owes	A machine that is safe for its intended use and for reasonably foreseeable misuse; a risk assessment; a technical file; instructions for use; a declaration of conformity and, in the European system, the CE marking	Suitable equipment for the work; keeping it in a safe condition; verifications and maintenance; training and information for operators; organisation of work; supply of protective equipment
Typical failure	A guard that can be removed with an ordinary tool; instructions omitting maintenance operations	A guard removed to gain productivity; an interlock deliberately defeated; an overdue verification

The second line of the last row deserves emphasis, because it is the situation you will most often meet in an Algerian plant. A machine that arrived compliant does not remain compliant. Interlocks are defeated, guards are removed and not replaced after maintenance, emergency stops are found unreachable behind stored material. None of this is the manufacturer's doing, and all of it falls to the employer — and in practice to the safety engineer, whose task is to detect it before an accident does.

1.7 Conformity, and what it does not guarantee

A declaration of conformity is a statement by the manufacturer, under his own responsibility, that the machine meets the applicable requirements. In the European system it accompanies the CE marking. For certain categories of higher-risk machinery, an independent body must be involved; for the rest, the manufacturer assesses conformity himself.

Three things follow, and they should temper the confidence that a marking inspires. Conformity is declared for the intended use stated by the manufacturer, not for any use. It is assessed at the moment of placing on the market, not later. And a substantial modification of a machine in service — a new function, a change of control system, a coupling with another machine — may create a new machine in law, with a new obligation of assessment falling this time on the one who modified it.

> *An examination question to expect: a plant couples two conforming machines with a conveyor and a common control system. Is the assembly conforming? No. The assembly is a new machine, and the one who made it bears the obligations of a manufacturer for it.*

Summary of the chapter

- The law states an obligation of result and is binding; the standard states the state of the art and is, in principle, voluntary.
- Applying a recognised standard confers a presumption of conformity and, in litigation, shifts the burden of proof.
- In Algeria the general obligation rests on Law 88-07; technical standards are adopted by IANOR, largely from international standards.
- Machinery on the European market moves from Directive 2006/42/EC to Regulation (EU) 2023/1230 on 20 January 2027, with no overlapping period.
- Standards are of three types: A basic, B generic, C machine-specific. A type C standard prevails over the others for the machine it covers.
- ISO 12100 prescribes an iterative process and a three-step order of risk reduction: design, then safeguarding, then information for use. The order is binding.
- The manufacturer owes a safe machine at the moment of placing on the market; the employer owes a safe machine throughout its working life. Most of what a safety engineer meets in a plant belongs to the second column.

Questions for self-check

1. A supplier tells you that his machine does not have to comply with any standard because standards are voluntary. What do you answer?

2. What is a presumption of conformity, and what does it change for the manufacturer if an accident occurs?

3. You find a type B standard and a type C standard giving different requirements for the same guard. Which do you apply, and why?

4. Why is information for use placed last in the order of risk reduction, and what would be wrong with using it first?

5. A machine bearing a valid declaration of conformity injures an operator during a cleaning operation. Does the declaration settle the question of responsibility? Explain.

6. Your plant couples two machines and adds a common control system. What obligations does this create, and for whom?

UNIVERSITY YAHIA FARES OF MEDEA · FACULTY OF TECHNOLOGY

Department of Process and Environmental Engineering

Chapter 2 — Terminology and Definitions

Safety of Industrial Installations and Equipment · L3 Industrial Hygiene and Safety

Weeks 3 and 4 · Lecture notes · Dr. A. C. Rahmani

Why a chapter on vocabulary

In ordinary speech, hazard and risk are interchangeable. In safety engineering they are not, and treating them as synonyms makes a risk assessment impossible: one cannot rank what one cannot distinguish. This chapter fixes the vocabulary of ISO 12100, which is the vocabulary used by every other standard in the course and by every conformity document you will ever read.

The chapter is short in content and demanding in precision. Learn the definitions exactly. In the examination, an answer that uses these terms loosely will be marked as wrong even where the underlying reasoning is right — for the good reason that in a written risk assessment, the loose use of these terms is what produces the wrong conclusion.

2.1 The five terms that must never be confused

Term	Definition	Example on a milling machine
Hazard	A potential source of harm. It exists whether or not anyone is present.	The rotating cutter
Hazardous situation	A circumstance in which a person is exposed to at least one hazard.	The operator has his hand in the working area while the cutter rotates
Hazardous event	An event that can cause harm.	The hand contacts the rotating cutter
Harm	Physical injury or damage to health.	Amputation of a finger
Risk	The combination of the probability of occurrence of harm and the severity of that harm.	High: severe injury, frequent exposure, little possibility of avoidance

Read the table downwards and the logic of the whole discipline appears. A hazard by itself injures no one — a cutter locked behind a fixed guard is a hazard that produces no risk. It is the exposure that creates the hazardous situation, the event that produces the harm, and the combination of probability and severity that constitutes the risk. Each of the three protective steps studied in the previous chapter acts at a different point of that sequence: design removes the hazard, safeguarding prevents the hazardous situation, information for use reduces the probability of the hazardous event.

2.2 The elements of risk

ISO 12100 estimates risk from the severity of the possible harm and the probability of its occurrence, that probability being itself broken into three elements. Every risk estimation method you will meet — matrices, risk graphs, numerical scoring — is a way of combining these four quantities.

Element	What is considered
Severity of harm	Nature of the injury, from a scratch to death; number of persons exposed;

Element	What is considered
	reversibility
Frequency and duration of exposure	How often and for how long a person is in the hazard zone; note that maintenance and cleaning often dominate here
Probability of occurrence of a hazardous event	Reliability data, accident history, human behaviour including reasonably foreseeable misuse
Possibility of avoiding or limiting harm	Who operates the machine, how quickly the hazard arises, whether the person can perceive it and withdraw

> *The last element is the one students forget. A hazard that arises slowly, on a machine operated by a trained person who can see it coming, does not carry the same risk as the same hazard arising in a fraction of a second on a machine operated by an untrained one. Two identical machines in two different plants may carry different risks, and the assessment must say so.*

2.3 Limits, intended use and foreseeable misuse

Before any hazard is identified, the limits of the machine are determined. Four families of limits are considered: use limits — intended use and reasonably foreseeable misuse, level of training required, exposure of other persons; space limits — range of movement, space required for installation and maintenance, interface with the power supply; time limits — foreseeable life of the machine and of its components, service intervals; and other limits, such as the properties of the material processed, the environment, or the required cleanliness.

Two of these terms deserve their own definition, because everything the manufacturer owes is fixed by them.

Term	Definition and comment
Intended use	The use of the machine in accordance with the information provided in the instructions. It is what the manufacturer designed for and declared.
Reasonably foreseeable misuse	The use of the machine in a way not intended by the designer, but which may result from readily predictable human behaviour. It is not any misuse imaginable: it is the misuse an experienced designer should have anticipated — an operator reaching over a guard to clear a jam rather than stopping the machine, a guard defeated to save time, a machine used by an untrained person.

The distinction has direct consequences. A manufacturer is not liable for absurd misuse, but he is required to design against predictable misuse. Since defeating an interlock to save time is entirely predictable, ISO 14119 requires interlocking devices to be designed so as to minimise the possibility of defeat, and a device that a screwdriver and a spare actuator can defeat does not meet the requirement.

2.4 The vocabulary of protective measures

The terms below designate the means by which risk is reduced. They are studied in detail in Chapter 4; here you learn to name them correctly.

Term	Definition
Protective measure	Any measure intended to achieve risk reduction, whether taken by the designer or by the user
Safeguard	A guard or a protective device
Guard	A physical barrier, part of the machine, specifically provided to give protection
Fixed guard	A guard kept in place either permanently or by fasteners that make removal impossible without tools

Term	Definition
Movable guard	A guard that can be opened without tools; it is normally associated with an interlocking device
Interlocking device	A device that prevents hazardous machine functions from operating while the guard is open, and stops them if it is opened
Guard locking device	A device that additionally keeps the guard closed and locked until the hazard has ceased — used where the machine takes time to stop
Protective device	A safeguard other than a guard: light curtain, pressure-sensitive mat, two-hand control device, enabling device
Emergency stop function	A function intended to avert or reduce a hazard, initiated by a single human action; it is complementary and never replaces a safeguard
Safety function	A function of a machine whose failure results in an immediate increase of the risk
Residual risk	The risk remaining after protective measures have been taken; it is the object of the information for use
Safe state	The state of the machine in which the hazard is absent — usually, but not always, the machine stopped

> *One misconception to correct now: an emergency stop is not a protective measure against a hazard that a guard should cover. It is a complementary measure for the situation that escapes the safeguards. A machine whose only protection is an emergency stop is an unguarded machine.*

2.5 The vocabulary of functional safety

These terms are studied in Chapter 5. They appear here so that you can read a technical datasheet from the beginning of the course, because they are printed on every safety component you will handle.

Term	Meaning in one sentence
Performance Level (PL)	A discrete level, from a to e, specifying the ability of the safety-related parts of a control system to perform a safety function under foreseeable conditions — ISO 13849-1
Required Performance Level (PLr)	The Performance Level the safety function must reach, determined from the risk before the control system is designed
Safety Integrity Level (SIL)	A discrete level, from 1 to 3 in machinery, expressing the same idea in the vocabulary of IEC 62061 and IEC 61508
Category	The classification of the architecture of a safety-related control system with respect to its behaviour in the event of a fault — B, 1, 2, 3, 4
MTTFD	Mean time to dangerous failure of a component or channel
Diagnostic coverage (DC)	The proportion of dangerous failures detected by the automatic diagnostics
Common cause failure (CCF)	Failures of several components resulting from a single cause, which defeat redundancy
Safety instrumented system (SIS)	An instrumented system implementing one or more safety functions in a process installation — IEC 61511
Proof test	A periodic test intended to reveal dangerous failures that the diagnostics do not detect

2.6 Bilingual glossary

The technical vocabulary of this field is used in English in datasheets and in French in most Algerian regulatory documents. You will need both. Learn this table.

English	Français	English	Français
Hazard	Phénomène dangereux	Guard	Protecteur
Hazardous situation	Situation dangereuse	Fixed guard	Protecteur fixe
Hazardous event	Événement dangereux	Movable guard	Protecteur mobile
Harm	Dommage	Interlocking device	Dispositif de verrouillage
Risk	Risque	Guard locking	Interverrouillage
Risk assessment	Appréciation du risque	Protective device	Dispositif de protection
Risk estimation	Estimation du risque	Light curtain	Barrière immatérielle
Risk evaluation	Évaluation du risque	Two-hand control	Commande bimanuelle
Risk reduction	Réduction du risque	Emergency stop	Arrêt d'urgence
Inherently safe design	Prévention intrinsèque	Safety distance	Distance de sécurité
Safeguarding	Protection	Hazard zone	Zone dangereuse
Information for use	Information pour l'utilisation	Safety function	Fonction de sécurité
Intended use	Usage normal	Residual risk	Risque résiduel
Reasonably foreseeable misuse	Mauvais usage raisonnablement prévisible	Safe state	État sûr

Summary of the chapter

— A hazard is a potential source of harm; it becomes a hazardous situation when a person is exposed, a hazardous event when harm can occur, and harm when it does.

— Risk combines the severity of harm with the probability of its occurrence, that probability resting on exposure, on the probability of the hazardous event, and on the possibility of avoidance.

— The limits of the machine are determined before hazards are identified: use, space, time, and others.

— Reasonably foreseeable misuse is part of what the designer must address; defeating an interlock to save time is foreseeable, and standards require design against it.

— A guard is a physical barrier; a protective device is a safeguard that is not a barrier; an emergency stop is complementary and never a substitute for either.

— Performance Level and Safety Integrity Level express the same idea — the ability of a control system to perform a safety function — in two different standards.

Questions for self-check

1. Define, in one sentence each and without using the other terms, hazard, hazardous situation and harm. Give one example of each on a machine you know.

2. Two identical presses are installed in two plants. Can the risk differ? Justify using the four elements of risk.

3. A worker climbs over a fence to retrieve a fallen part while the machine runs. Is this reasonably foreseeable misuse or not? What follows for the designer?

4. Why can an emergency stop device not be counted as the safeguard for a rotating tool?

5. What is a residual risk, and which of the three risk-reduction steps deals with it?

6. A supplier offers a component marked PL d and another marked SIL 2. What do these two markings tell you, and can they be compared?

Department of Process and Environmental Engineering

Chapter 3 — Safety of Installations

Safety of Industrial Installations and Equipment · L3 Industrial Hygiene and Safety

Weeks 5 to 7 · Lecture notes · Dr. A. C. Rahmani

From the machine to the installation

The previous chapters dealt with a machine: a bounded object, with an operator, a hazard zone and a guard. An installation is not a large machine. It is a set of equipment, pipework, storage and utilities, connected by flows of material and energy, operated by several people who do not see each other, and capable of harming persons who are not employed there at all. Three things change with the scale, and this chapter is organised around them.

The first is that the hazard is no longer contained in a zone: it travels. A leak becomes a cloud, a cloud finds an ignition source two hundred metres away, a fire on one vessel heats the vessel beside it. The second is that the accident sequence is long: an installation rarely fails in one step, which is both a danger, because the sequence can be missed, and an opportunity, because a long sequence can be interrupted at several points. The third is that the persons at risk include neighbours, and that changes the legal regime entirely.

3.1 The hazards of a process installation

Family	Origin	Typical consequence
Fire	Flammable liquid or gas released and ignited; pool fire, jet fire, flash fire	Thermal radiation, escalation to neighbouring equipment
Explosion	Confined vapour cloud, dust cloud in suspension, runaway reaction, mechanical rupture under pressure	Overpressure, projectiles, structural collapse
Toxic release	Loss of containment of a toxic gas or vapour	Effects at distance, on personnel and on population
Uncontrolled pressure	Overfilling, thermal expansion, blocked outlet, external fire on a vessel	Rupture, boiling liquid expanding vapour explosion
Loss of utilities	Failure of electrical supply, instrument air, cooling water, nitrogen	Loss of several protections at once — a common-cause failure at plant scale
Human and organisational	Work on the wrong line, isolation not verified, hot work permit not respected	Present in the causal chain of most major accidents

> *Note the fifth row. In a plant, the failure of one utility can defeat many independent-looking protections simultaneously. When you assess an installation, always ask what a loss of electrical power, of instrument air or of cooling water does to every protection you have just counted as independent.*

3.2 Inherently safer design at plant scale

The three-step method of ISO 12100 applies to installations too, and its first step has a well-established vocabulary in process safety. Four principles, in order of decreasing power.

Principle	Meaning	Example
Intensify	Reduce the quantity of hazardous material present	Continuous reaction with a small hold-up instead of a large batch reactor; smaller intermediate storage
Substitute	Replace a hazardous substance or process by a less hazardous one	A non-flammable solvent; a less toxic refrigerant
Attenuate	Use the hazardous material under less	Storage refrigerated at atmospheric pressure rather than

Principle	Meaning	Example
	severe conditions	liquefied under pressure; dilution
Simplify	Design out the sources of error and the need for added protection	Fewer manual interventions; equipment rated for the maximum pressure the source can deliver, so that a relief device is not needed

The last example deserves attention because it states the whole philosophy. A vessel designed to withstand the maximum pressure its source can deliver cannot be over-pressurised: the hazard has been removed, not protected against. Every protection added instead — a relief valve, an alarm, a trip — is a device that can fail, that must be tested, and that will one day be found isolated.

3.3 Layout, separation and safety zones

Layout is the cheapest safety measure available, and it is available only once — at the design stage. Once the plant is built, a separation distance that was not provided cannot be bought back at any price.

What separation achieves

- It limits escalation: a fire on one item does not heat the next beyond its resistance.
- It separates ignition sources from possible release points, which is the basis of hazardous-area classification.
- It preserves access: fire-fighting access, escape routes in at least two directions, and room to work without entering another hazard zone.
- It separates occupied buildings — control room, workshop, offices — from the process units, and orients them so that a blast does not reach a glazed façade head-on.

Hazardous-area classification

Where flammable gases, vapours or dusts may be present, the installation is divided into zones according to the likelihood that an explosive atmosphere occurs. The classification then governs what electrical and mechanical equipment may be installed in each zone.

Zone	Gases and vapours	Dusts
Zone 0 / 20	Explosive atmosphere present continuously or for long periods	Zone 20 — same criterion for a dust cloud
Zone 1 / 21	Likely to occur occasionally in normal operation	Zone 21
Zone 2 / 22	Not likely in normal operation, and if it occurs, only for a short period	Zone 22

> *A practical consequence you will meet in any plant: bringing a non-certified device — a mobile telephone, a camera, an ordinary drill — into a classified zone is not a formality violated, it is an ignition source introduced into a place where the atmosphere may be explosive. This is what a hot work permit exists to control.*

3.4 Layers of protection

An installation is protected not by one measure but by a series of independent layers, each capable of interrupting the accident sequence. Presenting them as concentric layers has a pedagogical virtue: it shows that the outer layers only limit consequences, and that everything worth doing is done in the inner ones.

Layer	Function	Examples
1 · Process design	Prevent the hazard from existing	Inherently safer design; equipment rated for the maximum credible pressure
2 · Basic process control	Keep the process within its normal	Regulation loops, normal operating procedures

Layer	Function	Examples
	envelope	
3 · Alarms and operator action	Alert and allow a human correction	High-level alarm with time for the operator to respond
4 · Safety instrumented system	Bring the process to a safe state automatically	High-high level trip closing the feed valve — Chapter 5
5 · Physical protection	Limit the consequence of a loss of containment	Relief valves, rupture discs, bunds and retention basins, flare
6 · Plant emergency response	Limit the damage once release has occurred	Fire-fighting, isolation, evacuation, internal emergency plan
7 · External emergency response	Protect the surrounding population	Public authorities, external emergency plan, sheltering or evacuation

Two rules govern the use of this model. A layer counts only if it is genuinely independent of the layers it is supposed to back up — an alarm and a trip taking their signal from the same sensor are one layer, not two. And the sum of the layers must be proportionate to the severity of the scenario: a scenario with off-site consequences cannot be left to an operator alarm.

3.5 Major-hazard installations

When the quantity of dangerous substance held on a site exceeds defined thresholds, the site changes regime. It becomes subject to authorisation, to a hazard study identifying the accident scenarios and their effect distances, to an internal emergency plan, and to land-use control around the site so that new dwellings are not built inside the effect distances. In Algeria this regime is carried by the classified-installations framework; in Europe it is the Seveso regime; the logic is the same everywhere.

The hazard study is the document the safety engineer will meet most often. It identifies the scenarios, estimates for each the distance at which given effect thresholds — thermal radiation, overpressure, toxic concentration — are reached, and states the measures that prevent or limit them. Its weakness, and the point on which it must be read critically, is that its conclusions depend entirely on the scenarios retained: a scenario not envisaged produces no effect distance and no measure.

3.6 Safe operation: the organisational layer

Most major accidents are not caused by the failure of a designed protection but by work performed on an installation that was believed to be in a state it was not in. Three procedures address that, and they are examinable.

Procedure	What it controls	Failure mode to know
Permit to work	Any non-routine work: hot work, entry, work on live systems	Permit issued for the wrong equipment, or conditions no longer valid when work starts
Isolation and lock-out	Separating the equipment from every energy and material source before work	Isolation by a single valve that leaks; energy stored in springs, capacitors, pressure or gravity not released
Management of change	Any modification of process, equipment, control or organisation	A "small" change made without assessment — the origin of a large share of process accidents

> *Lock-out is the point where machine safety and installation safety meet. The energy to be isolated is not only electrical: pressure, stored springs, suspended loads, residual heat and chemical inventory are all energy sources, and each requires its own proof of isolation before work begins.*

Summary of the chapter

- An installation differs from a machine in three ways: the hazard travels, the accident sequence is long, and third parties may be harmed.
- The hazard families are fire, explosion, toxic release, uncontrolled pressure, loss of utilities, and human and organisational failure.
- Inherently safer design at plant scale follows four principles in order: intensify, substitute, attenuate, simplify.
- Layout and separation are the cheapest safety measures, and are available only at the design stage.
- Hazardous areas are classified in zones according to the likelihood of an explosive atmosphere, and the classification governs the equipment admitted.
- Protection is organised in independent layers; a layer that shares a component with another is not independent.
- Above defined thresholds a site becomes a major-hazard installation, with a hazard study, an emergency plan and land-use control.
- Permit to work, isolation and lock-out, and management of change are the three procedures that fail most often, and they fail organisationally rather than technically.

Questions for self-check

1. Give one example, on an installation you know, of each of the four principles of inherently safer design.

2. Why can a separation distance not be added after construction? What is done instead, and at what cost?

3. An alarm and an automatic trip both use the same level transmitter. How many layers of protection do you count? Justify.

4. What does a loss of instrument air do to the protections of an installation? Name at least three consequences.

5. What is the principal weakness of a hazard study, and how do you read one critically?

6. List the energy sources that must be isolated before working on a stirred, heated, pressurised reactor.

UNIVERSITY YAHIA FARES OF MEDEA · FACULTY OF TECHNOLOGY

Department of Process and Environmental Engineering

Chapter 4 — Safety of Machinery and Equipment

Safety of Industrial Installations and Equipment · L3 Industrial Hygiene and Safety

Weeks 8 to 11 · Lecture notes · Dr. A. C. Rahmani

What this chapter is for

This is the technical core of the course, and the only chapter in which you will calculate. Everything here answers one question: a hazard zone exists and cannot be designed out, so how is the person kept out of it, or the machine stopped before the person arrives?

Two answers exist and they are combined. Keep the person out by distance or by a barrier — that is the safety distance and the guard. Or detect the approach and stop the machine in time — that is the protective device, and it introduces a calculation, because stopping takes time and the person keeps moving during that time.

4.1 Safety distances to prevent reaching the hazard zone

ISO 13857 gives the distances at which an upper or lower limb cannot reach a hazard zone. The standard works by tables, not by formula, and three configurations must be distinguished. The tables assume a

person who does not use a tool, a chair or a ladder, and who is not deliberately trying to defeat the safeguard — safety distances protect against reaching, not against determined defeat.

Configuration	What is tabulated	The variable that governs
Reaching over a protective structure	The distance to keep between the structure and the hazard zone	Height of the hazard zone, height of the structure, and the risk level
Reaching through a regular opening	The distance from the opening to the hazard zone	Size and shape of the opening — slot, square, round — and the limb that can pass: fingertip, finger, hand, arm
Reaching around, and lower limbs	The distance from the edge or the opening to the hazard zone	The part of the body that can pass through the opening

> *The practical consequence for a mesh guard: the smaller the opening, the closer to the hazard the guard may stand. This is why a fine mesh may be mounted near a rotating part while a coarse one must be placed far back — and why replacing a damaged fine mesh with the coarse mesh available in the store makes the guard non-compliant without anyone noticing.*

4.2 Positioning a protective device: the calculation

When the safeguard detects a person instead of barring the way, the machine must reach a safe state before the person reaches the hazard. ISO 13855 gives the minimum distance from the detection plane to the hazard zone.

$$S = (K \times T) + C$$

Symbol	Meaning	Value or determination
S	Minimum distance from the detection zone to the hazard zone, in millimetres	The result sought
K	Approach speed of the body or part of the body, in millimetres per second	2000 mm/s where the calculated S does not exceed 500 mm; 1600 mm/s may be used for larger distances, in accordance with the standard
T	Total stopping performance, in seconds	T = t1 + t2 : t1 the response time of the protective device and its control system; t2 the stopping time of the machine, measured, not assumed
C	Intrusion distance: how far the body can penetrate before detection	For an electro-sensitive device with detection capability d not exceeding 40 mm: C = 8 (d − 14), never less than zero

Worked example

A light curtain with a detection capability of 30 mm protects a press. The device and its relay respond in 30 ms; the press has been measured to stop in 250 ms.

T = 0.030 + 0.250 = 0.280 s

C = 8 × (30 − 14) = 128 mm

S = 2000 × 0.280 + 128 = 560 + 128 = 688 mm

The curtain must therefore stand at least 688 mm from the hazard zone. Two lessons follow. A slower machine needs a larger distance, so improving the brake is often cheaper than rebuilding the workstation. And a curtain with finer resolution reduces C — with d = 14 mm, C falls to zero and S becomes 560 mm — so resolution is bought back in floor space.

> *The single most frequent error in industry, and in examinations: taking t2 from the manufacturer's datasheet instead of measuring it. Brakes wear. The stopping time of a machine in service is not the stopping time of the same machine when new, and the distance calculated from the datasheet is then too short.*

4.3 Guards

A guard is a physical barrier that is part of the machine. ISO 14120 gives the general requirements: a guard must be robust, must not itself create a hazard — no shear points, no sharp edges — must resist the projections and the substances it is meant to contain, must allow the work to be done without being removed, and must permit maintenance if possible without being dismantled.

Type	Definition	Where it is appropriate
Fixed guard	Held in place permanently or by fasteners requiring a tool	Where access is not needed in normal operation — transmission parts, drives
Movable interlocking guard	Can be opened without a tool; opening stops the hazardous function	Where access is needed regularly: loading, adjustment, clearing
Interlocking guard with locking	Additionally kept locked until the hazard has ceased	Where the machine has run-down time, so the guard cannot be opened while parts still move
Adjustable guard	Fixed guard with an adjustable element set by the operator	Where the tool or the workpiece varies in size — the guard is only as good as the setting
Self-closing guard	Moved by the workpiece and returning automatically	Where the workpiece itself opens the passage it needs

4.4 Interlocking devices

ISO 14119 classifies interlocking devices and, above all, requires that they be designed to minimise the possibility of defeat in a reasonably foreseeable manner. That requirement exists because defeating an interlock to save time is a predictable human behaviour, not an exceptional one.

Type	Principle	Comment
Type 1	Mechanically actuated, uncoded — cam, plunger	Simple and robust; defeat is easy with a screwdriver
Type 2	Mechanically actuated, coded — tongue actuator	A spare actuator defeats it; spare actuators must be controlled
Type 3	Non-contact, uncoded — magnetic switch	A magnet defeats it
Type 4	Non-contact, coded — RFID transponder, uniquely coded	The highest level of coding; defeat requires the coded actuator itself

Guard locking deserves a separate word because two distinct principles exist and they fail in opposite ways. A device locked by spring force and released by power stays locked when power is lost; a device locked by power and released by spring opens when power is lost. The first protects the person from the machine, the second frees the person from an enclosure. Which is correct depends on whether the greater danger is entering a running machine or being trapped inside one — and that is a risk-assessment decision, not a catalogue decision.

4.5 Protective devices other than guards

Device	How it works	Limits to state
Electro-sensitive protective equipment (light curtain)	An optical beam array detects the intrusion of a body part and commands a stop	Detects passage, not presence: a person can pass through and stand behind the plane. Requires muting or blanking for material transfer, and both are frequent sources of defeat
Pressure-sensitive mat or edge	Detects the presence of a person by pressure	Detects presence but wears out and is often bypassed when faulty
Two-hand control device	The machine runs only while both hands	Protects the operator only, never a second

Device	How it works	Limits to state
	maintain the actuators, outside the hazard zone	person; must require simultaneous actuation within a short window to prevent tying one control down
Enabling device	A three-position switch: releasing or squeezing hard stops the machine	For work inside a hazard zone in a special mode; must be combined with reduced speed
Emergency stop device	Single human action bringing the machine to a stop	Complementary measure only, never a substitute for a guard

Emergency stop: what the standards require

ISO 13850 requires the emergency stop function to be available and operational at all times, to override all other functions, and not to create additional hazards. IEC 60204-1 defines the stop categories used to implement it.

Stop category	Description	Use
0	Immediate removal of power to the machine actuators	Where an uncontrolled stop is safe
1	Controlled stop, power retained to achieve the stop, then removed	Where an immediate power cut would itself create a hazard — a rotating mass, a raised load
2	Controlled stop with power retained at the end	Normal operational stop; not admissible for an emergency stop function

> *An emergency stop must be reachable from every operating position and along every access route, must remain latched once operated, and must require a deliberate action to reset — and the reset must not, by itself, restart the machine. A stop that restarts on reset is a well-known way of injuring the person who came to help.*

Summary of the chapter

— ISO 13857 gives, by tables, the distances at which a limb cannot reach a hazard zone, over a structure or through an opening.

— ISO 13855 gives the minimum positioning distance of a detecting device: $S = (K \times T) + C$.

— T is the sum of the device response time and the measured machine stopping time; taking the stopping time from the datasheet is the classic error.

— C is the intrusion distance; for an electro-sensitive device with $d \le 40$ mm, $C = 8\,(d - 14)$, not less than zero.

— Guards are fixed, movable and interlocking, interlocking with locking, adjustable or self-closing; each has a domain and none is universal.

— Interlocking devices are classified in four types by actuation and coding, and must be designed against foreseeable defeat.

— Protective devices — light curtains, mats, two-hand controls, enabling devices — each protect against something specific and must be stated with their limits.

— The emergency stop is a complementary measure. Stop categories 0 and 1 are admissible for it; category 2 is not.

Questions for self-check

1. A light curtain of resolution 14 mm protects a machine whose measured stopping time is 180 ms; the device responds in 20 ms. Calculate S.

2. The same machine, after two years of service, stops in 320 ms. What is the new S, and what does this tell you about periodic verification?

3. Why does a finer resolution allow the curtain to be placed closer to the hazard?

4. A workshop replaces a damaged fine mesh guard with a coarser mesh of the same dimensions. What has changed, and what must now be done?

5. On what grounds do you choose between a guard locked by spring and released by power, and the opposite arrangement?

6. Explain why a two-hand control device protects the operator but not his colleague, and what must be added where a second person may be present.

UNIVERSITY YAHIA FARES OF MEDEA · FACULTY OF TECHNOLOGY

Department of Process and Environmental Engineering

Chapter 5 — Functional Safety of Machines

Safety of Industrial Installations and Equipment · L3 Industrial Hygiene and Safety

Weeks 12 to 15 · Lecture notes · Dr. A. C. Rahmani

When safety depends on a control system

A fixed guard bolted over a drive protects by its presence: it has no failure mode other than being removed. As soon as protection depends on a sensor, a logic unit and an actuator — a guard that must be detected as closed, a light curtain that must command a stop — safety depends on a system that can fail. Functional safety is the discipline that quantifies how much one may rely on such a system.

The question it answers is not "does it work?" but "how often, and in what manner, does it fail dangerously?" A control system can fail in two directions. A safe failure stops the machine when it need not have stopped: it costs production. A dangerous failure leaves the machine running when it should have stopped: it costs a hand. The whole apparatus of this chapter exists to bound the second.

5.1 Safety functions

A safety function is a function whose failure results in an immediate increase of the risk. It is specified before any hardware is chosen, and its specification has a fixed form: what is detected, what is commanded, in what time, and to what state.

> *Example of a correctly written safety function: "When the loading gate is opened, the rotation of the spindle shall be stopped within 0.5 s and restarting shall be prevented while the gate is open." A specification that says "the gate shall be safe" is not a safety function and cannot be verified.*

5.2 Two standards, one idea

	ISO 13849-1:2023	**IEC 62061:2021**
Vocabulary	Performance Level, PL a to PL e	Safety Integrity Level, SIL 1 to SIL 3 in machinery
Object	Safety-related parts of control systems, any technology: electrical, hydraulic, pneumatic, mechanical	Safety-related control systems, electrical, electronic and programmable electronic
Determination of the target	Risk graph giving the required Performance Level PLr from severity, frequency of exposure and possibility of avoidance	Risk estimation giving the target SIL
Quantity used	Average probability of dangerous failure per hour, combined with the architecture Category, MTTFD, DC and CCF	Probability of dangerous failure per hour, with architectural constraints and systematic capability

The two standards express the same idea in two vocabularies, and a correspondence exists between the levels, since both rest on the same underlying probability of dangerous failure per hour. In practice a

machine builder chooses one framework and applies it consistently; the safety engineer must be able to read both, because components are marked in both.

5.3 Determining the required level

The required Performance Level is determined from the risk, before any component is selected. Three parameters are used, and they are the same three that appeared in Chapter 2.

Parameter	Levels	Meaning
S — severity of injury	S1 slight, reversible · S2 serious, irreversible, including death	What the injury would be if the safety function failed
F — frequency and duration of exposure	F1 seldom to less often, short duration · F2 frequent to continuous, long duration	How often a person is in the hazard zone
P — possibility of avoiding the hazard	P1 possible under specific conditions · P2 scarcely possible	Whether the person can perceive and withdraw

The combination of the three gives PLr from a to e. The direction of the result is intuitive and should be memorised: a serious injury, frequent exposure and no possibility of avoidance lead to PL e; a slight injury, rare exposure and a real possibility of avoidance lead to PL a.

5.4 What determines the level achieved

Once the target is known, the level actually achieved by a design is determined by four things. This is the part students find abstract; anchor it by remembering that each of the four answers a different question.

Element	Question it answers	Classes
Category (architecture)	What happens when a single fault occurs?	B and 1: a fault leads to loss of the safety function. 2: the function is tested at suitable intervals. 3: a single fault does not lead to loss of the function. 4: single faults are detected, and an accumulation of faults does not lead to loss of the function
MTTFD	How long before a channel fails dangerously, on average?	Low: 3 to less than 10 years · Medium: 10 to less than 30 years · High: 30 to 100 years
Diagnostic coverage DC	What proportion of dangerous failures is detected automatically?	None below 60 % · Low 60 to less than 90 % · Medium 90 to less than 99 % · High 99 % and above
Common cause failure CCF	Can one cause defeat both channels at once?	Assessed by a scoring list — separation, diversity, protection against over-voltage and temperature, competence

> *Why common cause failure matters more than students expect: two identical channels, from the same batch, in the same enclosure, sharing the same power supply, are not two independent channels. Redundancy that ignores common cause is arithmetic without engineering.*

5.5 Orders of magnitude

The levels correspond to bands of average probability of dangerous failure per hour. Knowing the bands lets you read a datasheet without a table.

Performance Level	Average probability of dangerous failure per hour	Approximate SIL correspondence
PL a	10^{-5} to less than 10^{-4}	no correspondence
PL b	3×10^{-6} to less than 10^{-5}	SIL 1
PL c	10^{-6} to less than 3×10^{-6}	SIL 1
PL d	10^{-7} to less than 10^{-6}	SIL 2

Performance Level	Average probability of dangerous failure per hour	Approximate SIL correspondence
PL e	10^{-8} to less than 10^{-7}	SIL 3

5.6 Safety-related control circuits in practice

Three practical points bridge the theory and the workshop.

Contactors and positively guided contacts

A contactor whose main contacts weld does not open when de-energised. A positively guided contact set — mechanically linked so that a normally closed auxiliary contact cannot close while a normally open main contact is welded — allows the fault to be detected by the logic. This is how a Category 3 or 4 architecture achieves fault detection in its output stage.

Safety relays and safety PLCs

A safety relay unit implements a fixed function — emergency stop monitoring, guard monitoring, two-hand control — with internal redundancy and self-testing. A safety PLC does the same in software, with a certified operating system, and is used where the number of functions makes discrete units impractical. In both cases the safety function must not be programmed in the standard control PLC, which is designed for availability rather than for the detection of its own dangerous failures.

Restart and reset

Three requirements are examinable and are frequently violated in service. The restoration of the guard must not by itself restart the machine. The reset device must be located where the whole hazard zone is visible. And an automatic restart after a power failure must be prevented unless the risk assessment has explicitly permitted it.

5.7 Safety instrumented systems in process installations

In a process installation the same logic takes another name. A safety instrumented function is implemented by a safety instrumented system, and IEC 61511 organises it as a life cycle rather than as a product.

Phase	Content
Hazard and risk analysis	Identify the scenarios and decide which require an instrumented protection
Allocation and SIL determination	Determine the required integrity level of each safety instrumented function
Safety requirements specification	Write, for each function, what is measured, the trip point, the action, the process safety time and the safe state
Design and engineering	Select sensors, logic solver and final elements; determine the architecture and the redundancy
Installation, commissioning and validation	Verify that what was built performs what was specified
Operation and maintenance	Proof testing at the defined interval; management of bypasses and overrides
Modification and decommissioning	Any change re-enters the cycle at the appropriate phase

Two notions deserve to be retained beyond the list. The process safety time is the interval between the deviation and the occurrence of harm if nothing acts; the system must complete its action well within it. And the proof test exists because dangerous failures that the diagnostics do not detect accumulate silently: an untested safety instrumented function does not keep the integrity level it was designed for — it loses it gradually, and no alarm announces the loss.

> *The bypass is where this chapter meets reality. A trip that is bypassed for a start-up and not restored is a protection that exists on paper and not in the plant. Every bypass must be authorised, recorded, time-limited*

> *and verified on removal — and the register of active bypasses is one of the most informative documents a safety engineer can ask to see.*

Summary of the chapter

- Functional safety quantifies the reliability of a protection that depends on a control system; a dangerous failure leaves the machine running when it should stop.
- A safety function is specified before hardware: what is detected, what is commanded, in what time, to what state.
- ISO 13849-1 uses Performance Levels a to e; IEC 62061 uses Safety Integrity Levels; both rest on the probability of dangerous failure per hour.
- The required level is determined from severity, frequency of exposure and possibility of avoidance — the same three parameters as in risk estimation.
- The level achieved depends on the architecture Category, on MTTFD, on diagnostic coverage, and on the assessment of common cause failure.
- Positively guided contacts allow output faults to be detected; safety functions are not programmed in a standard control PLC.
- In process installations, IEC 61511 organises safety instrumented systems as a life cycle, with proof testing and bypass control as its weakest points in practice.

Questions for self-check

1. Write a correctly specified safety function for the loading gate of a mixer, and explain why "the gate must be safe" is not one.

2. A machine causes a serious irreversible injury, exposure is continuous and avoidance is scarcely possible. What is the required Performance Level, and why?

3. Two identical channels share one power supply and sit in the same enclosure. What does this do to the level achieved, and under what heading is it assessed?

4. What is a positively guided contact, and what fault does it allow the logic to detect?

5. Why must a safety function not be programmed in the standard control PLC?

6. A safety instrumented function has not been proof-tested for four years. Does it still have the integrity level for which it was designed? Explain.

UNIVERSITY YAHIA FARES OF MEDEA · FACULTY OF TECHNOLOGY

Department of Process and Environmental Engineering

Tutorial Sheets — TD 1 to TD 5

Safety of Industrial Installations and Equipment · L3 Industrial Hygiene and Safety

One sheet per chapter · Dr. A. C. Rahmani

Each sheet is designed for one tutorial session of 1 h 30. Exercises marked GRADED are submitted through the Moodle Assignment activity and count towards the continuous assessment.

TD 1 — The normative framework (week 2)

Exercise 1. A supplier delivers a machine with a declaration of conformity. During commissioning your plant adds a robot loader and a common control system. Draw up, in one page, the list of obligations this creates and state who bears each. GRADED.

Exercise 2. For a machine of your choosing, find whether a type C standard exists. State how you searched, and what you conclude if none exists.

Exercise 3. Take three requirements from any safety document available to you. Classify each as a legal obligation or a technical recommendation, and justify.

Exercise 4. Explain, in five lines, what a plant loses by treating the standard as optional, even where the law does not cite it.

TD 2 — Terminology (week 4)

Exercise 1. For a bench drill, a bread slicer and a conveyor, fill a table with: hazard, hazardous situation, hazardous event, possible harm, and an estimate of risk using the four elements.

Exercise 2. Classify ten statements provided by the lecturer as intended use or reasonably foreseeable misuse, and justify each in one line.

Exercise 3. Rewrite three badly worded risk statements so that each uses the vocabulary of ISO 12100 correctly. GRADED.

Exercise 4. Two identical machines, two plants, two different risks: build the case and identify which of the four elements differs.

TD 3 — Installations (week 7)

Exercise 1. On a simplified flow diagram supplied by the lecturer, identify the hazard families present and mark the points at which a loss of containment could occur.

Exercise 2. For the same diagram, list the protection layers and state, for each, whether it is genuinely independent of the others. Identify at least one false independence.

Exercise 3. Apply the four principles of inherently safer design to one unit of the diagram, and propose one change per principle.

Exercise 4. Write the isolation list for maintenance on a stirred, heated, pressurised reactor: every energy and material source, and the proof required for each. GRADED.

TD 4 — Machinery safeguarding (week 10)

Exercise 1. Calculate S for three cases supplied by the lecturer, varying resolution and stopping time. Present the results in a table and comment on the sensitivity of S to each variable.

Exercise 2. A press is measured with a stopping time 60 % longer than at commissioning. Recalculate S and state the two possible remedies with their cost implications.

Exercise 3. Select and justify a safeguard for four workstations described by the lecturer, and state the limits of the device chosen in each case. GRADED.

Exercise 4. Examine a real machine in the workshop. Photograph its safeguards, identify their type, and state one non-conformity or one weakness with the standard that applies.

TD 5 — Functional safety (week 14)

Exercise 1. Write the specification of three safety functions for a machine described by the lecturer, in the required form.

Exercise 2. Determine the required Performance Level for each, from S, F and P, and justify each parameter.

Exercise 3. Read three component datasheets and extract PL, Category, MTTFD and DC. State whether the combination meets the target. GRADED.

Exercise 4. A bypass register from a plant is supplied. Identify which entries are irregular and explain what each irregularity risks.

> *Advice for the graded exercises: mark on the justification, not on the result. A correct value of S with no statement of the assumptions is worth less than a wrong value accompanied by a clear reasoning, because in practice it is the assumptions that are audited.*

Appendix A — Formulas and quantities

Every quantity used in this course, with its unit, its origin and the precaution attached to it. Learn the precautions: in practice it is the assumptions that are audited, not the arithmetic.

Quantity	Relation or definition	Unit and precaution
Front intensity	I = H · w · r	kW/m. H in kJ/kg, w in kg/m², r in m/s. w is the fuel consumed, not the fuel present
Flame length	Power relation with intensity	m. Empirical, with wide dispersion; useful to translate intensity into an observable quantity
Minimum positioning distance	S = (K × T) + C	mm. The central calculation of Chapter 4
Approach speed K	Standard value	mm/s. 2000 where the calculated S does not exceed 500 mm; 1600 may be used beyond, per ISO 13855
Total stopping performance T	T = t1 + t2	s. t1 device and control response; t2 machine stopping time, measured on the machine in service
Intrusion distance C	C = 8 (d − 14) for d ≤ 40 mm	mm. Never less than zero. d is the detection capability of the device
Performance Level	Discrete level a to e	Bands of average probability of dangerous failure per hour — ISO 13849-1
Safety Integrity Level	Discrete level 1 to 3 in machinery	Same underlying quantity, vocabulary of IEC 62061 and IEC 61508
MTTFD	Mean time to dangerous failure	years. Low 3 to <10, medium 10 to <30, high 30 to 100
Diagnostic coverage DC	Proportion of dangerous failures detected	%. None <60, low 60 to <90, medium 90 to <99, high ≥99

Bands of probability of dangerous failure per hour

Performance Level	Probability per hour	Approximate SIL
PL a	10^{-5} to less than 10^{-4}	—
PL b	3×10^{-6} to less than 10^{-5}	SIL 1
PL c	10^{-6} to less than 3×10^{-6}	SIL 1
PL d	10^{-7} to less than 10^{-6}	SIL 2
PL e	10^{-8} to less than 10^{-7}	SIL 3

Worked example, for reference

A light curtain of detection capability 30 mm protects a press. The device and its relay respond in 30 ms; the press has been measured to stop in 250 ms.

T = 0.030 + 0.250 = 0.280 s

C = 8 × (30 − 14) = 128 mm

S = 2000 × 0.280 + 128 = 688 mm

With a detection capability of 14 mm, C falls to zero and S becomes 560 mm. Resolution is bought back in floor space.

> *The most frequent error, in industry and in examinations: taking the stopping time from the manufacturer's datasheet instead of measuring it. Brakes wear. The stopping time of a machine in service is not that of the same machine when new, and the distance calculated from the datasheet is then too short.*

Appendix B — Bilingual glossary

The technical vocabulary of this field is used in English in datasheets and in French in most Algerian regulatory documents. You will need both.

English	Français	English	Français
Hazard	Phénomène dangereux	Guard	Protecteur
Hazardous situation	Situation dangereuse	Fixed guard	Protecteur fixe
Hazardous event	Événement dangereux	Movable guard	Protecteur mobile
Harm	Dommage	Interlocking device	Dispositif de verrouillage
Risk	Risque	Guard locking	Interverrouillage
Risk assessment	Appréciation du risque	Protective device	Dispositif de protection
Risk estimation	Estimation du risque	Light curtain	Barrière immatérielle
Risk evaluation	Évaluation du risque	Two-hand control	Commande bimanuelle
Risk reduction	Réduction du risque	Emergency stop	Arrêt d'urgence
Inherently safe design	Prévention intrinsèque	Safety distance	Distance de sécurité
Safeguarding	Protection	Hazard zone	Zone dangereuse
Information for use	Information pour l'utilisation	Safety function	Fonction de sécurité
Intended use	Usage normal	Residual risk	Risque résiduel
Foreseeable misuse	Mauvais usage prévisible	Safe state	État sûr
Loss of containment	Perte de confinement	Layer of protection	Couche de protection
Hazardous area	Zone à risque d'explosion	Permit to work	Permis de travail
Lock-out	Consignation	Management of change	Gestion des modifications
Proof test	Test périodique	Bypass, override	Dérogation, inhibition
Dangerous failure	Défaillance dangereuse	Redundancy	Redondance
Common cause failure	Défaillance de cause commune	Process safety time	Temps de sécurité du procédé

Appendix C — Standards and references

Algerian legal framework

- Law no. 88-07 of 26 January 1988 on occupational health, safety and medicine — the general obligations of the employer.
- Law no. 03-10 of 19 July 2003 on environmental protection in the framework of sustainable development — classified installations.
- IANOR — Institut algérien de normalisation, which adopts international standards as Algerian standards under the prefix NA.

International standards used in this course

Reference	Title	Type
ISO 12100:2010	Safety of machinery: general principles for design, risk assessment and risk reduction	A
ISO 13857:2019	Safety distances to prevent hazard zones being reached by upper and lower limbs	B1
ISO 13855:2010	Positioning of safeguards with respect to the approach speeds of parts of the human body	B1
ISO 14120:2015	Guards: general requirements for the design and construction of fixed and movable guards	B2
ISO 14119:2013	Interlocking devices associated with guards: principles for design and selection	B2
ISO 13850:2015	Emergency stop function: principles for design	B2
IEC 60204-1:2016	Electrical equipment of machines: general requirements	B1
ISO 13849-1:2023	Safety-related parts of control systems, part 1: general principles for design	B1
IEC 62061:2021	Functional safety of safety-related control systems	B1
IEC 61508 / 61511	Functional safety of E/E/PE safety-related systems, and its application to the process industry	—

> *These standards are copyrighted documents and cannot be redistributed. Ask at the university library whether an institutional subscription gives you access. What you need in order to cite a requirement correctly is the reference itself.*

European legislation

- Directive 2006/42/EC on machinery — in force until 20 January 2027.
- Regulation (EU) 2023/1230 on machinery — adopted 14 June 2023, applies from 20 January 2027, on which date Directive 2006/42/EC is repealed. No overlapping transition period.

Freely available guides

- Schneider Electric, machine safety guide — cited by the official course programme.
- INRS (France), technical publications on machinery safety, guards and safety distances — freely downloadable, in French.
- European Commission, guide to the application of the Machinery Directive — useful for the vocabulary of conformity even outside the European Union.

Appendix D — Preparing for the examination

The examination covers the five chapters and counts for 60 % of the final mark. It tests the method rather than recall, and the distribution of the questions reflects the weight of the chapters in the programme.

What is asked, chapter by chapter

Chapter	What you are expected to do	Typical form
1	Classify a requirement as legal or normative; state who is bound; apply the hierarchy of standards; order the three steps of risk reduction	Short questions, one case to analyse
2	Use the five terms exactly; estimate a risk from its four elements; distinguish intended use from foreseeable misuse	Definitions, and a table to complete on a given machine
3	Identify hazard families; apply the four principles of inherently safer design; count protection layers and detect false independence	A flow diagram to analyse
4	Calculate S; recalculate after a change of parameter; select and justify a safeguard, stating its limits	Calculation, with the assumptions to be stated
5	Write a safety function; determine a required Performance Level from S, F and P; read a datasheet	Specification to write, level to justify

How answers are marked

On the justification, not on the result. A correct value of S with no statement of the assumptions is worth less than an imperfect value accompanied by clear reasoning — because in practice it is the assumptions that are audited, and a number without them cannot be defended.

Three faults are penalised every year, and all three are avoidable. Inverting the order of the three steps of risk reduction. Using hazard and risk as synonyms. And presenting the emergency stop as the safeguard for a hazard that a guard should cover.

A revision method that works

— Read the summary at the end of each chapter first, not the chapter. If a bullet point means nothing to you, go back to the section it comes from — and only to that section.

— Answer the six self-check questions in writing, without looking at the text. Writing reveals what re-reading conceals.

— Redo the calculation of Chapter 4 three times, changing one variable each time, until the direction of each change is obvious to you without computing.

— Take one machine you can actually see — in a workshop, at home, in a bakery — and run the whole method on it: limits, hazards, risk, three steps. One machine done properly teaches more than five chapters read twice.

> *The last item is the one that separates the students who pass from those who understand. The examination can be passed by revision; the profession cannot be practised without having applied the method at least once to something real.*

Appendix E — Indicative answers to the self-check questions

These are indicative answers, not model answers to be reproduced. What is marked is the reasoning: an answer that reaches the same conclusion by another route, and states its assumptions, is worth as much.

Chapter 1 — The normative framework

1. A supplier tells you that his machine does not have to comply with any standard because standards are voluntary. What do you answer?

That he is formally right and practically wrong. A standard is voluntary in principle, but applying a recognised one confers a presumption of conformity, and departing from it places on him the burden of demonstrating an equivalent level of safety. In litigation after an accident, the standard is the yardstick against which his design will be measured.

2. What is a presumption of conformity, and what does it change if an accident occurs?

It is the presumption that a manufacturer who applied a recognised standard has met the corresponding legal requirement. It reverses the burden of proof: the authority must show non-compliance, rather than the manufacturer having to prove compliance.

3. A type B and a type C standard give different requirements for the same guard. Which do you apply?

The type C standard. It is specific to the machine or family concerned, and where it departs from a type A or B standard it prevails.

4. Why is information for use placed last, and what would be wrong with using it first?

Because a warning placed where a design change or a guard was possible transfers the risk from the designer to the operator. Step 3 is legitimate only for the residual risk that survives steps 1 and 2.

5. A machine with a valid declaration of conformity injures an operator during cleaning. Does the declaration settle responsibility?

No. Conformity is declared for the intended use stated by the manufacturer and assessed at the moment of placing on the market. If cleaning was not covered by the instructions, or if the machine was modified or badly maintained since, the question remains entirely open.

6. Your plant couples two machines and adds a common control system. What obligations does this create, and for whom?

The assembly constitutes a new machine. The obligations of a manufacturer — risk assessment, technical file, instructions, declaration of conformity — fall on the one who made the assembly, that is to say the plant.

Chapter 2 — Terminology

1. Define hazard, hazardous situation and harm without using the other terms.

A hazard is a potential source of harm; it exists whether or not anyone is present. A hazardous situation is a circumstance in which a person is exposed to a hazard. Harm is physical injury or damage to health.

2. Two identical presses in two plants. Can the risk differ?

Yes. Severity may be identical while exposure, the probability of a hazardous event and the possibility of avoidance all differ — different work organisation, different training, different maintenance practice. The risk is a property of the situation, not of the machine alone.

3. A worker climbs over a fence to retrieve a fallen part while the machine runs. Foreseeable misuse or not?

Foreseeable. It results from readily predictable human behaviour, and the designer must address it — by preventing access, by detecting it, or by removing the reason to do it.

4. Why can an emergency stop not be the safeguard for a rotating tool?

Because it acts only after a human being has perceived the danger and reacted, which is too late for a hazard that produces harm on contact. It is a complementary measure for what escapes the safeguards, not a substitute for them.

5. What is residual risk, and which step deals with it?

The risk remaining after protective measures have been taken. It is the object of step 3, information for use.

6. A component marked PL d and another marked SIL 2: what do these tell you, and can they be compared?

Both express the ability of a safety-related control system to perform a safety function, in the vocabularies of ISO 13849-1 and IEC 62061 respectively. They rest on the same underlying probability of dangerous failure per hour, and PL d corresponds approximately to SIL 2.

Chapter 3 — Installations

1. Give an example of each of the four principles of inherently safer design.

Intensify: reduce the intermediate storage volume. Substitute: replace a flammable solvent by a non-flammable one. Attenuate: store refrigerated at atmospheric pressure rather than liquefied under pressure. Simplify: rate the vessel for the maximum pressure its source can deliver, so that no relief device is required.

2. Why can a separation distance not be added after construction?

Because it consumes land already occupied by equipment, roads and buildings. What is done instead is compensation by added protections — fire-fighting, thermal shielding, detection — each of which costs money every year and can fail, whereas the distance would have cost nothing after the initial layout.

3. An alarm and a trip on the same transmitter: how many layers?

One. Independence is the condition for counting a layer, and a shared sensor defeats it. A single failure of the transmitter removes both.

4. What does a loss of instrument air do to the protections of an installation?

It can close or open every pneumatically actuated valve at once according to their fail position, disable pneumatic control loops, and defeat several protections simultaneously. It is a common-cause failure at plant scale, and it must be examined whenever independence is claimed.

5. What is the principal weakness of a hazard study?

That its conclusions depend entirely on the scenarios retained. A scenario not envisaged produces no effect distance and no measure, and nothing in the document signals the omission. It is read critically by asking what is absent, not by checking what is present.

6. Energy sources to isolate on a stirred, heated, pressurised reactor.

Electrical supply to the agitator and to the instruments; residual pressure; thermal energy in the jacket and in the mass; stored mechanical energy in the agitator inertia and in any spring-loaded valve; chemical inventory remaining in the vessel and in the connected lines; and gravity for anything suspended or elevated.

Chapter 4 — Machinery safeguarding

1. Light curtain of resolution 14 mm, stopping time 180 ms, device response 20 ms. Calculate S.

$T = 0.020 + 0.180 = 0.200$ s. $C = 8\,(14 - 14) = 0$ mm. $S = 2000 \times 0.200 + 0 = 400$ mm.

2. The same machine now stops in 320 ms. New S, and what does this tell you?

$T = 0.020 + 0.320 = 0.340$ s, $S = 2000 \times 0.340 = 680$ mm. The installation, compliant at commissioning, no longer is: the curtain stands 400 mm from the hazard where 680 are now required. Stopping time must be measured periodically, and the measurement is a verification obligation of the employer.

3. Why does a finer resolution allow the curtain to be placed closer?

Because C = 8 (d − 14) decreases with d and reaches zero at 14 mm. A finer detection capability means the body is detected earlier in its penetration, so less distance is needed to compensate for the intrusion.

4. A coarse mesh replaces a damaged fine mesh of the same dimensions. What has changed?

The opening size has increased, so a larger part of the limb can pass, so the distance required by ISO 13857 between the guard and the hazard zone has increased. The guard, unchanged in position, is now too close: it must be moved back or the correct mesh fitted.

5. On what grounds do you choose between spring-locked and power-locked guard locking?

On the risk assessment. Spring-locked and power-released stays locked on power failure, which protects the person from entering a machine that may still be dangerous. Power-locked and spring-released opens on power failure, which frees a person who might be trapped inside. The choice depends on which of the two dangers is greater on that machine.

6. Why does a two-hand control protect the operator but not his colleague?

Because it guarantees only that the hands of the person operating it are outside the hazard zone. It says nothing about anyone else. Where a second person may be present, the two-hand control must be combined with a guard or a presence-detecting device.

Chapter 5 — Functional safety

1. Write a safety function for the loading gate of a mixer.

"When the loading gate is opened, the rotation of the mixing blades shall be stopped within 1 s, and restarting shall be prevented while the gate is open." It is a safety function because it states what is detected, what is commanded, in what time and to what state. "The gate must be safe" states none of the four and cannot be verified.

2. Serious irreversible injury, continuous exposure, avoidance scarcely possible. Required Performance Level?

PL e. The three parameters are at their most severe: S2, F2 and P2. It is the highest level, and it will require a Category 3 or 4 architecture with high diagnostic coverage.

3. Two identical channels, one power supply, one enclosure. Effect on the level achieved?

The redundancy is largely illusory: a single cause — loss of supply, over-voltage, temperature, a common manufacturing defect — can defeat both. It is assessed under common cause failure, by a scoring list covering separation, diversity, protection and competence, and a poor score caps the level achievable whatever the architecture.

4. What is a positively guided contact, and what fault does it reveal?

A set of contacts mechanically linked so that a normally closed auxiliary contact cannot close while a normally open main contact is welded. It allows the logic to detect a welded contactor, which would otherwise leave the machine powered after a stop command.

5. Why must a safety function not be programmed in the standard control PLC?

Because that PLC is designed for availability and for process control, not for the detection of its own dangerous failures. It has neither the internal redundancy, nor the self-testing, nor the certified operating system required, and a dangerous failure of its processor or of its outputs would remain undetected.

6. A safety instrumented function not proof-tested for four years: does it keep its integrity level?

No. Dangerous failures that the automatic diagnostics do not detect accumulate silently between tests. The average probability of failure on demand rises continuously with the interval, and the function loses the level for which it was designed without any alarm announcing it. The proof test interval is part of the design, not a maintenance convenience.

> *If your answer differs from the one given here but rests on stated assumptions and on a named standard, it is a good answer. If it reaches the same conclusion without any justification, it is not.*