SEMINARIO TECNICO

ASSOLOMBARDA

Milano

4 dicembre 2013

LA MANOMISSIONE DEI CIRCUITI DI SICUREZZA NELLE MACCHINE

Relatore

Dott. Ing. Federico Dosio

DIRETTIVA 2006/42/CE Art. 1.1.2: principio di integrazione della sicurezza

Riduzione del pericolo alla fonte

↓

Adozione di protezioni

↓

Istruzioni per l'uso

Art. 1.1.2 comma c)

"In sede di progettazione e di costruzione della macchina, nonché all'atto della redazione delle istruzioni il fabbricante, o il suo mandatario, deve prendere in considerazione non solo l'uso previsto della macchina, ma anche l'uso scorretto ragionevolmente prevedibile."

Le protezioni includono i circuiti di comando per applicazioni di sicurezza

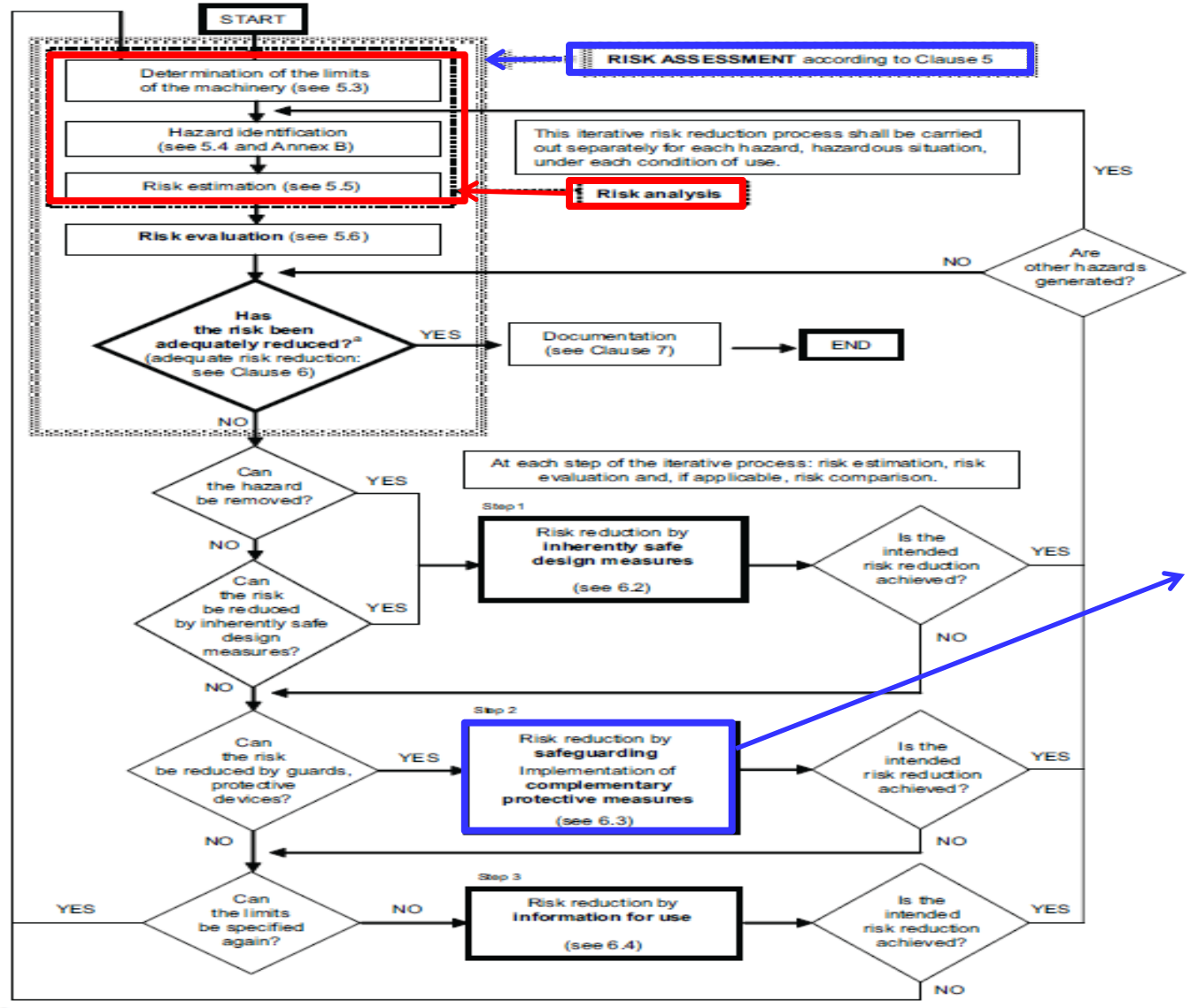
Prescrizioni della Direttiva 2006/42/CE: art. 1.2.1“ Sicurezza ed affidabilità dei sistemi di comando”

“I sistemi di comando devono essere progettati e costruiti in modo da evitare l’insorgere di situazioni pericolose. In ogni caso devono essere progettati e costruiti in modo tale che:

- resistano alle previste sollecitazioni di servizio e agli influssi esterni,
- un'avaria nell'hardware o nel software del sistema di comando non crei situazioni pericolose
- errori della logica del sistema di comando non creino situazioni pericolose,
- errori umani ragionevolmente prevedibili nelle manovre non creino situazioni pericolose.
Particolare attenzione richiede quanto segue:
— la macchina non deve avviarsi in modo inatteso,
— i parametri della macchina non devono cambiare in modo incontrollato, quando tale cambiamento può portare a situazioni pericolose,
……

L’applicazione delle pertinenti norme armonizzate consente di soddisfare il suddetto

NORMA UNI EN ISO 12100: procedura riduzione del rischio



[a] The first time the question is asked, it is answered by the result of the initial risk assessment.

L'applicazione delle misure di protezione include l'uso dei circuiti di sicurezza

Normative riguardanti i circuiti di sicurezza

Serie CEI EN 61508: Sicurezza funzionale dei sistemi elettrici elettroni, elettronici ed elettronici programmabili per applicazioni di sicurezza.

CEI EN 62061: Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza

UNI EN ISO 13849-1: Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione

UNI EN ISO 13849-2: Parti dei sistemi di comando legate alla sicurezza - Parte 2: Validazione

Le Norme CEI EN 62061, UNI EN ISO 13849-1 e UNI EN ISO 13849-1 sono armonizzate per la Direttiva 2006/42/CE art. 1.2.1“ Sicurezza ed affidabilità dei sistemi di comando”

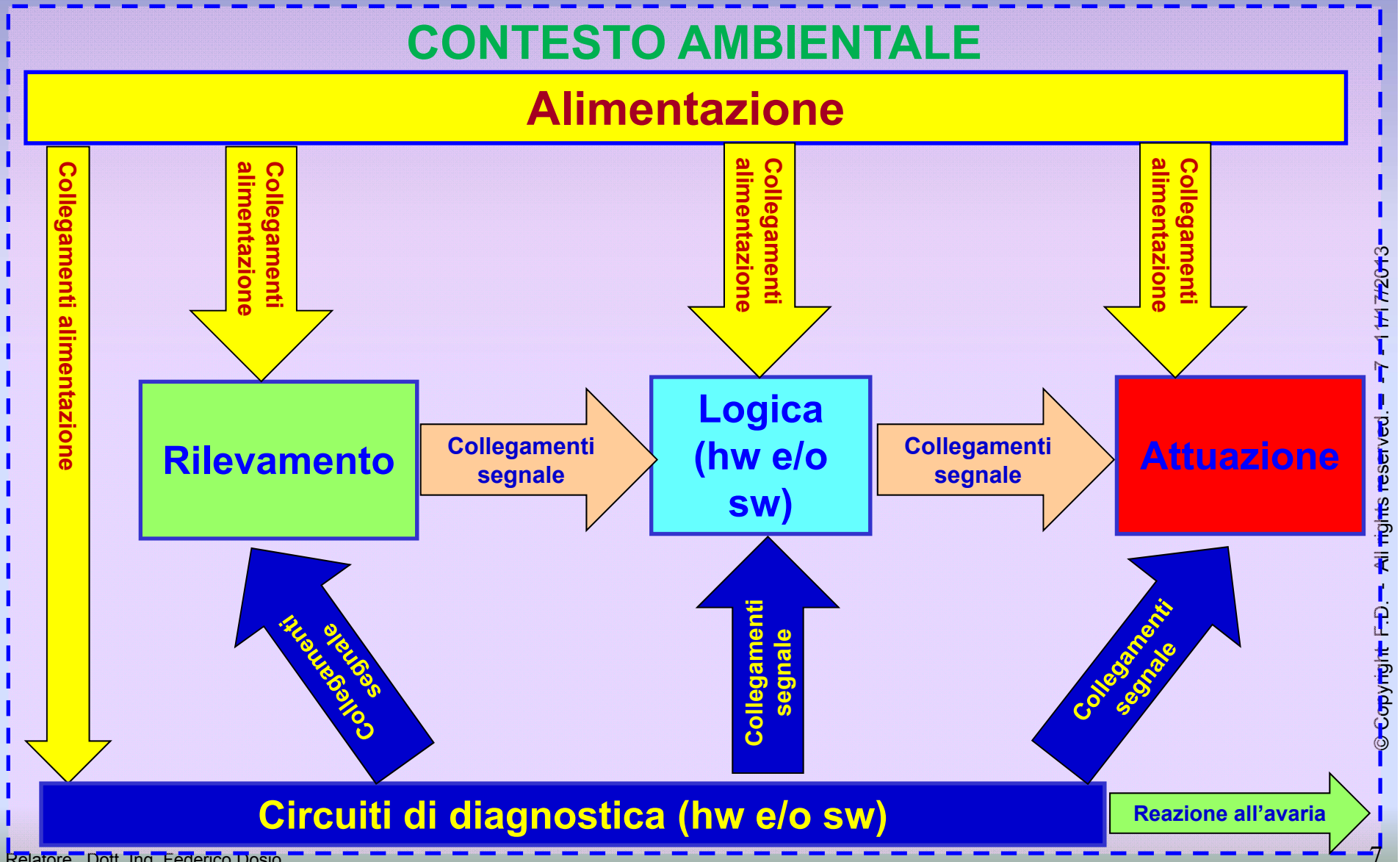
CIRCUITI DI SICUREZZA: definizioni

- **CEI EN 62061 art. 3.2.4 - SRECS (Safety-Related Electrical Control System)**
  "Sistema elettrico di controllo di una macchina il cui guasto può produrre un immediato aumento del rischio"

- **UNI EN ISO 13849-1 art. 3.1.1 - Parti del sistema di controllo legate alla sicurezza SRP/CS**
  "Parte del sistema di controllo che risponde a segnali di ingresso relativi alla sicurezza e genera segnali di uscita relativi alla sicurezza"

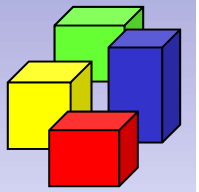
Un circuito di sicurezza include tutte le parti che guastandosi possono causare il suo malfunzionamento

STRUTTURA GENERALE DI UN CIRCUITO DI SICUREZZA



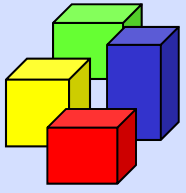
ASPETTI SALIENTI DEI CIRCUITI DI SICUREZZA

ASPETTI LEGATI ALLA PROGETTAZIONE



- Scelta della architettura del circuito idonea al rischio da ridurre
- Accurata scelta dei componenti idonei alla specifica applicazione di sicurezza
- Accurata analisi ed eliminazione delle cause di guasto comune
- Adeguata scrittura del sw di sicurezza su hw di sicurezza
- Prevenzione dell'uso scorretto ragionevolmente prevedibile

ASPETTI LEGATI ALL'USO



- Rispetto dei limiti d'uso
- Rispetto delle prescrizioni di manutenzione in base alle istruzioni fornite dal costruttore del circuito di sicurezza
- Uso del circuito nell'ambito del suo tempo di vita e di quello dei suoi componenti

PARAMETRI RELATIVI AI CIRCUITI DI SICUREZZA

CEI EN 62061

- Tasso di guasto in modalità pericolosa λ
- Tempo medio al guasto pericoloso MTTFd (derivato dal B10d per i componenti elettromeccanici)
- Copertura diagnostica DC e intervallo T2 del test delle funzioni diagnostiche
- Parametro T1 (minore tra il proof test ed il tempo di vita del circuito)
- Suscettibilità β

UNI EN ISO 13849-1

- Tempo medio al guasto pericoloso MTTFd (derivato dal B10d per i componenti elettromeccanici)
- Copertura diagnostica DCavg del circuito mediante funzioni diagnostiche
- Determinazione del parametro CCF

Il livello di integrità dei circuiti è quantificato in:
- Safety Integrity Level (SIL) per la Norma CEI EN 62061
- Performance Level (PL) per la Norma UNI EN ISO 13849-1

PARAMETRI RELATIVI AI CIRCUITI DI SICUREZZA

CEI EN 62061

Tabella 3 – Livelli di integrità della sicurezza: valore di guasto da raggiungere per le SRCF

Livello di integrità della sicurezza	Probabilità di un Guasto pericoloso per Ora (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTA Quando l'integrità della sicurezza prescritta di una SRCF è inferiore a SIL 1, dovrebbero essere rispettate almeno le prescrizioni della categoria B della ISO 13849-1.

UNI EN ISO 13849-1

PL	Probabilità media di guasto pericoloso per ora 1/h
a	$\geq 10^{-5}$ fino a $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ fino a $< 10^{-5}$
c	$\geq 10^{-6}$ fino a $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ fino a $< 10^{-6}$
e	$\geq 10^{-8}$ fino a $< 10^{-7}$
Nota Oltre alla probabilità media di guasto pericoloso per ora, anche altre misure sono necessarie per raggiungere il PL.	

PL	SIL
a	
b	SIL 1
c	
d	SIL 2
e	SIL 3

Tabella di equivalenza ai soli fini del PFH_D

Il calcolo del PFH_D è funzione dei parametri , β, MTTFd, B10d, λ, T1, T2, DCavg, utilizzati nelle rispettive norme

MANOMISSIONE DEI CIRCUITI DI SICUREZZA

MANOMISSIONE

MANOMISSIONE VOLONTARIA

Alterazione di una parte del circuito di sicurezza per ottenere vantaggi in termini di produttività

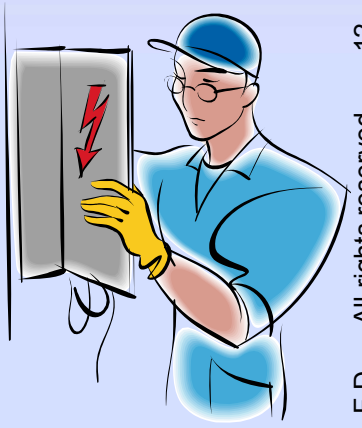
MANOMISSIONE INVOLONTARIA

- Sostituzione di parti guaste del circuito di sicurezza con altre incompatibili con il progetto del circuito
o
- alterazione delle condizioni in cui opera il circuito di sicurezza

MANOMISSIONE DEI CIRCUITI DI SICUREZZA

ESEMPI DI MANOMISSIONE INVOLONTARIA

- Sostituzione di un interruttore di sicurezza con un interruttore di minore caratteristica di MTTFd o B10
- Aggiunta di un ulteriore elemento di sicurezza nel circuito causando il decadimento del PL o il SIL originale
- Sostituzione di un variatore di velocità completo di funzione STO, SLS o SS1 con altro variatore con funzioni di sicurezza che garantiscono un PL o SIL inferiore
- Sostituzione di un contattore con altro di marca diversa e diverso parametro B10
- Modifica delle condizioni in cui opera il circuito



MANOMISSIONE DEI CIRCUITI DI SICUREZZA

ESEMPI DI MANOMISSIONE VOLONTARIA

- Elusione di un interruttore di sicurezza
- Manomissione del circuito elettrico nel quadro di comando e controllo per escluderne il funzionamento permanentemente o temporaneamente
- Modifica del sw di sicurezza
- Effettuare il by-pass delle uscite di sicurezza
- Smontare o orientare in modo diverso le barriere di sicurezza per consentire l'ingresso in zona pericolosa senza il loro intervento

ERRORI DI PROGETTAZIONE DEI CIRCUITI DI SICUREZZA

- **Errata errata scelta della tipologia di dispositivo di interblocco associato ai ripari**
- **Uso sw di sicurezza con libero accesso in programmazione**
- **Consentire all'utente l'uso di parametrizzazione del sw di sicurezza con parametri variabili tali da portare a condizioni non sicure**
- **Consentire il facile smontaggio ed elusione di determinati dispositivi di sicurezza in campo**
- **Eccedere nelle misure di sicurezza tali da limitare l'osservazione del ciclo di lavoro e conseguente incentivazione della manomissione.**

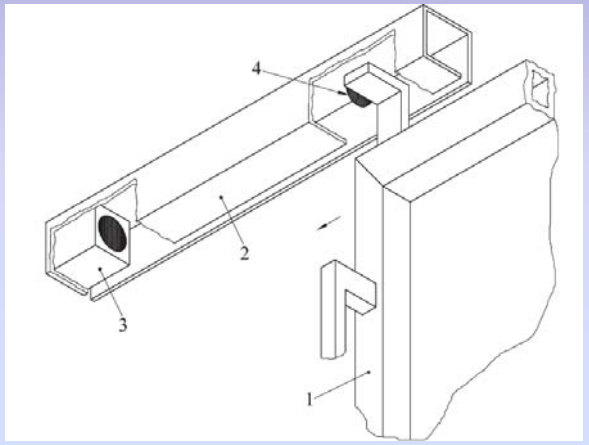
NORMA UNI EN 1088

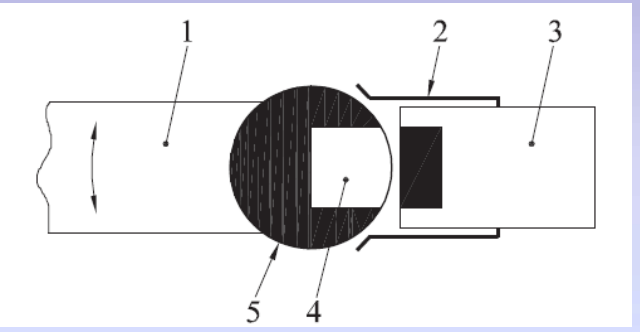
UNI EN 1088 (in futuro UNI EN ISO 14119): Sicurezza del macchinario - Dispositivi di interblocco associati ai ripari - Principi di progettazione e di scelta

- **Indica il tipo di dispositivo di interblocco appropriato per diverse tipologie di applicazione**
- **indica pregi e difetti di ciascuna tipologia di dispositivo di interblocco**
- **Indica alcune modalità per impedire l'elusione degli interblocchi**

NORMA UNI EN 1088

Esempi di misure contro l'elusione





Ulteriori misure contro l'elusione

- Usare rivetti o viti con testa fresata dopo l'installazione
- Usare sw con password di accesso
- Usare sensori codificati
- Sigillare i morsetti per evitare la modifica dei cablaggi

MANOMISSIONE DEI CIRCUITI DI SICUREZZA: Sanzioni

D.Lgs. 81/2008 art. 20 Obblighi dei lavoratori

"…. I lavoratori devono in particolare: ……

***c)** utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto e, nonché i dispositivi di sicurezza;*

***d)** utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;*

***e)** segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), …….;*

***f)** non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;*

***g)** non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;*

SANZIONI (art. 59 D.Lgs. 81/2008)

Arresto fino a 1 mese o ammenda da 200 Euro a 600 Euro oltre a ulteriori azioni penali nel caso in cui le corrispondenti violazioni abbiano causato danni alle persone

SEMINARIO TECNICO

ASSOLOMBARDA

Milano

4 dicembre 2013

LA MANOMISSIONE DEI CIRCUITI DI SICUREZZA NELLE MACCHINE

Grazie per l'attenzione

Relatore

Dott. Ing. Federico Dosio