GÉPEK KIBERBIZTONSÁGA
PROGRAM - 2026.12.16.

Dátum	**2026.12.16. (szerda)**
Képzés megnevezése	**Gépek kiberbiztonsága**
Helyszín	Online tréning (MS Teams)
A képzés célja	Megismertetni a gépek kiberbiztonságára vonatkozó jogszabályi környezetet (2023/1230/EU Géprendelet, kitekintéssel a Cyber Resilience Act-ra is) valamint a kapcsolódó szabványos követelményeket – vizsgálat bemutatása példa segítségével! A részletes program a következő oldalon található.
Amire nem fog kiterjedni	Az új jogszabályi követelményekhez egyelőre nem állnak rendelkezésre harmonizált szabványok. A képzés anyagát a jogi előírások és a jelenlegi szabványtervezetek alapján állítottuk össze!
Jelentkezés	**Online formában 2026.12.11-ig!** A jelentkezési lapot **ide kattintva** éred el.
A képzés időtartama	1 nap
Menetrend	9:00-tól kb. 16:00-ig tart a képzés, közben rövid szünetek és egy hosszabb ebédszünet. Kérjük, hogy a kezdés előtt 5-10 perccel jelentkezz be!
Szükséges alapismeretek	Nincsenek szükséges alapismeretek.
Kinek ajánljuk?	• Ipari gépek, gépegyüttesek tervezőinek, gyártóinak és integrátorainak (egyedi és sorozatgyártás esetén egyaránt) • Gépek átalakítóinak, karbantartóinak • Ipari vezérlések, biztonsági funkciók (SRP/CS) tervezőinek • Ellenőrzést, validálást végző szakembereknek
Tréning díja?	124.000 Ft + ÁFA / fő
Mit tartalmaz a díj?	• Egy fő számára a részvételi lehetőséget, letölthető anyagokat, valamint az előadás anyagát elektronikus formában is.
Kedvezmények?	• **Hazai mikrovállalkozások*** **25%** kedvezményre jogosultak a fenti díjból! *Kedvezményre jogosító kód:* ***MK25*** Ettől eltérő kedvezményekkel hírleveleinkben vagy együttműködő partnereink meghívóiban találkozhat. Minden esetben az Önt megillető legmagasabb kedvezményt vesszük figyelembe! (A kedvezmények nem összevonhatóak!) *Mikrovállalkozás: 10 fő alatti létszám és évi 2 m€ alatti forgalom
Egyéb feltételek	Az elhangzott program (beleértve az esetleges kérdéseket, kommenteket) rögzítésre kerülhet, amelyen a résztvevők is szerepelhetnek. A jelentkezésükkel ezt elfogadják, a készült felvételek felhasználásához hozzájárulnak, azokkal kapcsolatban semmilyen követelést nem támasztanak!
Adatszolgáltatási kötelezettség felnőttképzés esetén	A bejelentés és engedély alapján végezhető felnőttképzési tevékenységgel kapcsolatban a felnőttképzőknek adatszolgáltatási kötelezettségük van, melyet a felnőttképzési adatszolgáltatási rendszeren (FAR) keresztül kell teljesíteniük. Ebből adódóan a képzésen résztvevőknek adatszolgáltatási kötelezettségük van, melyet egy online adatlap kitöltésével teljesíthetnek, amelynek elérési linkjét a képzést megelőzően küldjük ki.
Lemondási feltételek	A részvételt a tréning megtartása előtti 4 naptári nappal lehet lemondani, ellenkező esetben a szervező jogosult a teljes részvételi díjat kiszámlázni/megtartani.

GÉPEK KIBERBIZTONSÁGA
PROGRAM - 2026.12.16.

MODUL MEGNEVEZÉSE	MODUL CÉLJA	MODUL TARTALMA
Bevezető és alapkérdések tisztázása	A gépekre vonatkozó műszaki szabályozási háttér és fogalmak, definíciók, alkalmazási terület körülhatárolása	• alapfogalmak • jogszabályok és szabványok szerepe • CE-jelölés fő lépései géptervezők és üzemeltetők számára • kiberbiztonság általában • OT, ipari kiberbiztonság • a biztonság kettős természete
Ipari gépek kiberbiztonságára vonatkozó jogszabályok és szabványok	A gépek kiberbiztonságára vonatkozó jogszabályok és szabványok beazonosítása, rövid áttekintése, összefüggéseik bemutatása és fontosabb dátumok, várható változások; Géprendelet előírásainak és a CRA követelményeinek bemutatása ismertetése	• Kibertörvény (NIS2) – 2022/2555/EU • Géprendelet (MR) – 2023/1230/EU • Kiberreziliencia rendelet (CRA) – 2024/2847/EU • prEN 50742, IEC 62443-x, EN 40000-x • jogszabályok, szabványok kapcsolatai • új, kiberbiztonsági relevanciájú Alapvető Egészségvédelmi és Biztonsági Követelmények (EHSR) és kapcsolódó további követelmények a CRA alapján
Kiberbiztonsági kontextus és fenyegetettség-felmérés	Kiberbiztonsági kontextus meghatározásának, szempontjainak áttekintés; a kiberbiztonsági fenyegetettségfelmérés folyamatának bemutatása	• ISO 12100 szerinti kockázatfelmérés és az ISO 13849-1 szerinti biztonsági funkciók specifikációinak összefüggése a kiberbiztonsággal • kiberbiztonsági kontextus elemei • zónák és csatornák • szempontok és módszertan
Biztonsági szintek	A prEN 50742 szerint Safety Related Security Level (SRSL) és az IEC 62443-x szerinti Security Level (SL) fogalmainak, meghatározási módjainak bemutatása	• szintek meghatározásának módszerei • tényezők magyarázata (AP, EL, WoO, AC) • SRSL / SL szintek és definíciók
Kiberbiztonsági követelmények	Biztonsági szinttől függő és általános kiberbiztonsági követelmények bemutatása	• a követelmények kategóriái és magyarázatai a prEN 50742 és az IEC 62443-x alapján • kriptográfia • információgyűjtés • jogosulatlan módosítások elleni védelem • szoftververziók és a konfiguráció azonosítása • azonosítás és jogosultságok • hozzáférések kezelés • rendszerintegritás • adatok bizalmassága • adatáramlás korlátozása • eseménykezelés • erőforrások hozzáférhetősége
Megfelelőségértékelési eljárás	Az alkalmazható megfelelőségértékelési modulok és kiválasztási szabályainak áttekintése	• Új Jogszabályi Keretrendszer (NLF) • Géprendelet előírásai • kitekintés a CRA előírásaira