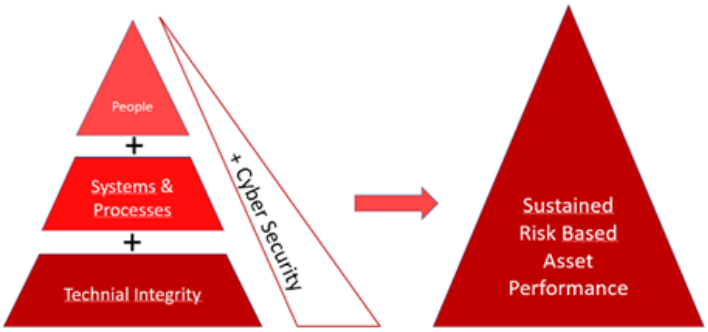
TÜV AUSTRIA Belgium nodigt u uit

Zijn al uw systemen voldoende beveiligd tegen inbreuken van buitenaf?

Uitnodiging tot ons Digitaal Event rond Veiligheid in de Industry 4.0—KLIK HIER



Tot voor 30 jaar geleden waren de meeste veiligheidsconcepten in de industrie alleen gericht op de technische integriteit. Zo'n 20 jaar geleden ontstond het besef dat Asset Performance and Safety beinvloed worden door processen en systemen, in combinatie met de technische integriteit.

Vervolgens werd erkend dat menselijke factoren (menselijk gedrag, cultuur, leiderschap en management, training, groepsgedrag, gewoonten) een grote impact hadden op veiligheid en prestaties. Gangbare aannames voor risicobeheer zijn dat tot 80% van alle veiligheids- en prestatie-incidenten menselijke factoren als oorzaak hebben.

Met het opkomen van Industrie 4.0 en het (Industrial) Internet of Things, is Cyber Security een wezenlijke factor geworden in het raamwerk van Asset Safety & Performance

De boodschap:

Het is belangrijk om te begrijpen dat integriteitsverlies ten gevolge van Cyber Criminaliteit een grote impact kan hebben op veiligheid en prestaties van uw installaties. Cyberincidenten kunnen hun oorzaak hebben in menselijke factoren (1), in systeem fouten (2) en via directe impact op technische integriteit (3).

ONZE AGENDA VOOR 29 APRIL

1. De uitdagingen met betrekking to Veiligheid in de industrie ten gevolge van Industrie 4.0 en Cyber Crime.
2. De 4 factoren van Asset Performance
3. De Mythes m.b.t. Cyber Crime in de Industrie
4. Wat kan TÜV AUSTRIA voor u hierin betekenen?
5. De TÜV AUSTRIA aanpak




1—(nalatigheid van het personeel)
2—(wachtwoord management, onvoldoende cyberveiligheidsmaatregelen, zoals Fire Walls, isolatie van systemen, enz.)
3—(IIoT maakt hardware direct kwetsbaar voor cyberaanvallen)