QR-koodi teollisuudessa

Mika Karaila, Valmet

QR-koodi on kameralla luettava digitaalinen ruutukoodi (QR == Quick Response). Koodi voi sisältää pelkkää tekstiä, url-linkki, tai ihmisen käyntikortin (lähteet: https://fi.wikipedia.org/wiki/QR-koodi#Rakenne,_virheenkorjaus_ja_ominaisuudet ja https://en.wikipedia.org/wiki/QR_code). Laitteet joissa on kamera voivat helposti lukea QR-koodin ja uusimmat älypuhelimet tukevat suoraan kamerasovelluksella jo QR-koodin tunnistamista.

Teollisuudessa QR-koodi ei korvaa mutta tekee konekilvestä digitaalisen. Kaikki tieto on julkista luettavissa kameralla, joka osaa purkaa QR koodin. Metallisessa konekilvessä on laitteen positio (tag), sarjanumero sekä malli. Koska nämä tiedot voi ihminen lukea niin samat tiedot voidaan laittaa luettavaksi QR-koodista.

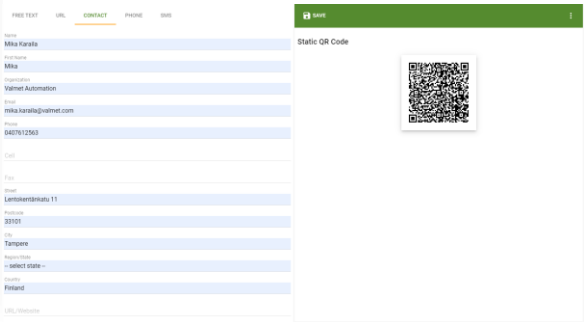
Vaihtoehtona olisi käyttää SQR Secure QR-koodia, mutta tämä vaatii, että sovelluksella on avain salatun koodin purkamiseen. Tämä estää laajan käytön, joten parempi on käyttää yksinkertaista julkista tekstuaalista tietoa, jotta tietoa voidaan hyödyntää mahdollisimman laajasti.

Käytännön huomioitavaa: likaisuus, valaistus, sijoitus, veden kestävyys, koko (pienelle alalle ei saada mahtumaan paljon tietoa, vaikka QR-koodiin voi tallettaa paljon tekstiä (max 4296 merkkiä).

Alla olevassa esimerkissä käytetään tekstuaalista formaattia ja QR-koodin koko on hieman isompi, jotta sen voi helposti lukea hieman kauempaa.

Esimerkki: FREE TEXT
TAG: 123FIC-98765
SERIALNUMBER: 123456789
MODEL: X989877

Kuva 1 Käyntikortti QR-koodina



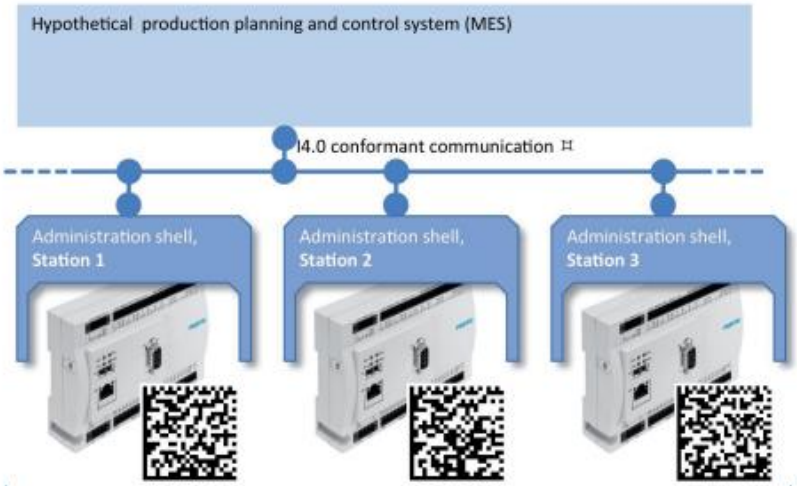
Kuva 2 Konekilpi QR-koodina

Tulevaisuudessa QR-koodin ensin yleistyessä voidaan saada hyviä sovelluksia, joiden avulla saadaan avattua dokumentaatio, huolto historia tai muuta laitteeseen liittyvää tietoa. Sovellus hakee oikean tiedon annetuilla tiedoilla ja näin myös se tekee tarvittavat tunnistautumiset sekä salaa tarvittaessa liikenteen sovelluksen ja tiedon / dokumentaation hakemisessa palvelimelta.

Uutena kilpailevana vaihtoehtona voi olla NFC-tarra, jota koskettamalla älypuhelin saa luettua tiedot NFC sirulta. Tässäkin on samat tarpeet ja haastavuudet kuin kamerapohjaisessa QR-koodissa. NFC:n tietoja voidaan päivittää kirjoittamalla uudet tiedot tarralle, jos sitä ei ole kirjoituslukittu.

QR koodin uhat ovat kuitenkin olemassa julkisten paikkojen koodeihin on voitu upottaa vahingollista koodia. QR koodi voi lisätä kontaktin ja soittaa siihen, tehdä maksusiirron, ilmoittaa käyttäjän paikkatiedon ja muita mahdollisia on esitetty liitteessä [1]. QR-koodin haavoittuvuutta on tarkastetu myös viitteissä [2] ja [3]. Tehtaan sisäiset QR-koodit on syytä tehdä niin, että niitä ei voida muuttaa (laserilla metallille poltettu kuva) tai kopioida ilman että se on selvästi huomattavissa.

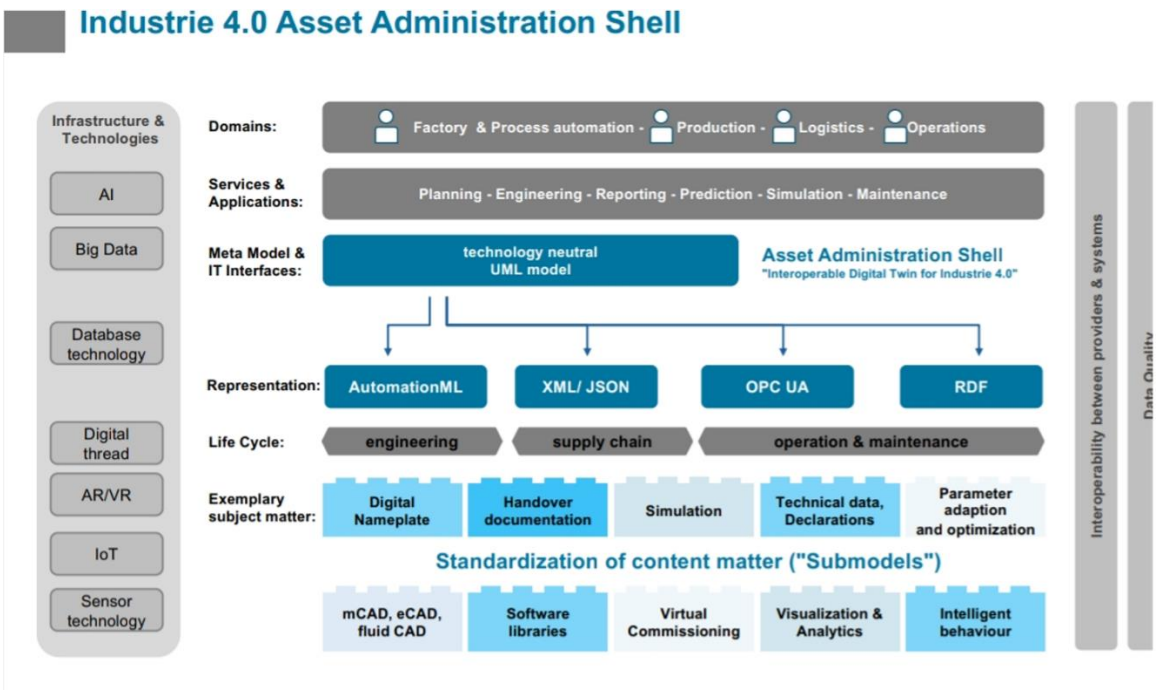
Figure 8: Identification in an example scenario



		Asset administration shell		
		Station 1	Station 2	Station 3
DF header	Asset administration shell ID	http://www.zvei.de/demo/11232322	http://www.zvei.de/demo/11232342	http://www.zvei.de/demo/11282322
	ID(s) of asset(s)	[http://pk.festo.com/3S7PLFDRS35]	[http://pk.festo.com/3S7PL9X6K32]	[http://pk.festo.com/3S7PLFNCKDZ]
DF body	ID SM "MES connection"	Type: ADA011 Instance: http://www.zvei.de/demo/2368473473829	ADA011 Instance: http://www.zvei.de/demo/1366423771829	ADA011 Instance: http://www.zvei.de/demo/8364423571326
	ID SM "Energy efficiency"	ADA012 [..]	ADA012 [..]	ADA012 [..]
	ID SM "Drilling"	ADA013 [..]	ADA013 [..]	ADA013 [..]
	ID TM "Documentation"	ADA014 [..]	ADA014 [..]	ADA014 [..]

Source: ZVEI

Standardisointi on edennyt OPC UA:n kautta ja digitaalinen konekilpi huomioitu [4]. Tätä voidaan käyttää edelleen kun uusi laitteiden hallintaan liittyvä ”Asset Administration Shell” saadaan käyttöön [5]. Alla siihen liittyvä kuva.



Viitteet

[1] Tarkistettu 5.10.2020 https://threatpost.com/qr-codes-sneaky-security-threat/159757/

[2] Tarkistettu 3.3.2022 https://www.helpnetsecurity.com/2020/09/17/qr-code-security-concerns/

[3] Tarkistettu 3.3. 2022
https://www.researchgate.net/publication/263146774_QR_Code_Security_A_Survey_of_Attacks_and_Challenges_for_Usable_Security

[4] Tarkistettu 3.3.2022
https://reference.opcfoundation.org/v104/DI/v102/ObjectTypes/IVendorNameplateType/

[5] Tarkistettu 3.3.2022I:
https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Asset_Administration_Shell/ZVEI_WP_Verwaltungschale_Englisch_Download_03.04.17.pdf

Tämä on liite kirjaan:
Automaation tietoturva – Kriittisen tuotannon turvaaminen
ISBN: 978-952-5183-58-0, ISSN 1455-6502, SAS julkaisusarja nro 51, © Suomen Automaatioseura ry,
www.automaatioseura.fi/AutomaationTietoturva