POSITION PAPER

Federal Association Food inspectors in Germany

BVLK

ENFIT INTERNATIONAL ASSOCIATION - SUPPLY CHAIN SAFETY

FOOD DEFENSE

Ensuring food safety at all levels - reliably protecting food from manipulation or sabotage during transport

Protection of critical infrastructure

The security situation in the world has changed dramatically. The current acts of sabotage on Nord Stream I/II and Deutsche Bahn make it clear how vulnerable our critical infrastructure is. To protect the critical infrastructure, which also includes food production and food transport, there is an urgent need for effective and standardized solutions that help prevent sabotage or manipulation.

FOOD DEFENSE - Initial situation

After the terrorist attacks on September 11, 2001 in the USA, the "Homeland Security Presidential Directive 9 of the USA" identified agriculture, food production and food transport as critical infrastructure and specific measures to protect against manipulation, sabotage and terrorist attacks were developed.

The USDA's Food Safety and Inspection Service defines "food defense" as "protecting food from intentional adulteration (tampering) with biological, chemical, physical, or radiological agents." This term also includes terms such as “bioterrorism” and “counterterrorism”* (*FDA FOOD DEFENSE Acronymus, Abbreviations and Definition).

These requirements were then translated into certification standards such as E.g.: IFS, BRC and FSSC 22000 included. All standards state that both the hazard analysis and the assessment of the associated risks are to be defined by the food producer himself, and therefore only basic recommendations are given.

In order to define their own FOOD Defense requirements, producers in the "IFS-International Featured Standard" are recommended to consider the following general questions that are directly related to the loading, unloading and transport of food, view.

These essentially include:

Are transport vehicles sealed (secured with lead seals) / locked?

Do the drivers have the appropriate authorizations?

How is it ensured that drivers cannot carry out any manipulation or contamination during loading and unloading?

Is it ensured that drivers only stay in defined areas during loading and unloading?

What entry controls are applied to drivers?

Are the transport companies part of the supplier approval process?

Are there delivery and shipping schedules?

Are unaccepted or delayed deliveries investigated?

Are goods taken back? If so, how are they managed?

Is it possible to verify the integrity of the product chain (chain of custody) for raw materials?

Are employees made aware of and trained in relation to product protection?

Are employees able to recognize manipulations?

Which physical and digital security devices are used?

FOOD Defense. Application in practice

The above questions, which are very general, show a basic direction for FOOD Defense, but also that they are not very suitable for specific instructions and organizational measures that go beyond your own production.

Why? FOOD defense measures that seem sensible and correct for a producer and its production are no longer suitable and safe when it comes to the complex networking of different stakeholders in the transport chain (supply chain).

This applies in particular to the transport of unpackaged raw materials and food in food transport containers. Here, the companies involved in the transport chain (loader, unloader and cleaning stations) are constantly changing, since one transport container is used for different products in order to avoid empty runs. In practice, this means that constantly changing companies come together with different interpretations and solutions on how food defense is implemented and that each company creates its own system and organizational measures.

Stakeholders involved in the transport chain / supply chain

- Producer of raw materials or semi-finished goods. Primary production (loader, check-in control, sealing, securing with seals and it's documentation)
- Producer of finished products. Secondary production (unloader, check-in control, checking whether transport containers are closed and sealed. Comparison with documentation)
- Logistics service providers (storage/ depot/ storage containers. Transport with their own transport containers or transport containers from subcontractors. Should ensure that their own or third-party transport containers are equipped with effective security devices and that the number and position of the seals is known)
- Transport company (transport with own transport containers or transport containers from subcontractors. Should ensure that own or third-party transport containers are equipped with effective security devices and that the number and position of the seals is known)
- Cleaning stations (cleaning of transport containers on behalf of the logistics or transport company and according to their specifications. Closing and securing)
- Repair, inspection of transport containers (installation of effective security systems at the relevant positions that are to be secured with seals)
- Driver. Loading and unloading. Transport (identification, check-in security, authorizations, responsibility)
- Employees in cleaning stations (management, cleaning staff, security, responsibility)

Because each producer defines and applies individual food defense requirements, this inevitably means that the complex networking and responsibility of all stakeholders involved in transport is not taken into account.

It is particularly frightening that most stakeholders, primarily the food companies, assume that a mature and effective system already exists and that the interfaces for the transfer of danger and risk are sufficiently defined. On closer examination in practice, one comes to the conclusion that those involved feel safe and that the current system offers an open and vulnerable flank to terrorism, manipulation or sabotage.

BVLK and ENFIT - Food Defense from a new perspective

As early as 2008, ENFIT therefore created the first international ENFIT guideline “Transport of raw materials and foodstuffs in transport containers”.

The trigger for the formation of the working group was an accumulation of cases of contamination in the food industry, which was obviously related to the transport, insufficient cleaning of the transport containers and thus poor transport hygiene, a lack of standards and a lack of training for the employees involved, as well as incomplete and incorrect documentation of the processes.

The acts of sabotage by Nord Stream I/II and Deutsche Bahn show how important it is to protect the critical infrastructure and thus the special protection of the food chain and food transport. A long-standing and successful cooperation between the two associations ENFIT and BVLK is now followed by a joint catalog of requirements to protect the critical infrastructure of food transport.

Our demands:

1. Synchronized Food Defense security and organization procedures

Development of a recommendation by the European Commission to comply with synchronized food defense security and organization procedures, including all companies involved in the transport chain, with reference to existing relevant regulations, such as: VO (EC) No. 178/2002 - food safety, food business operators, VO (EG) No. 852/2004 Hygiene Regulation, LMHV Food Hygiene Regulation, etc.

2. Employee training in industry, logistics and cleaning stations

Uniform training standard to raise awareness among employees of companies involved in transport logistics (loading, unloading, cleaning of transport containers):

o Food and raw material producers/ industry

o Logistics and transport

o cleaning stations

o Storage and depots

o Repair/ inspection/ testing

3. Guide/Certification for Instructors/Trainers

Development of a uniform food defense training standard for the training of trainers with proof of certification and regular updating.

4. Definition of responsibilities and control measures

Awareness of the staff. Who has which tasks and responsibilities

a. Drivers (logistics and transport companies)
b. Cleaning station staff (management and cleaners)
c. Loader and unloader personnel (QM, site management, logistics, purchasing, gatekeepers and security guards)
d. Personnel in container testing centers according to DIN 10 502-1 (experts)

5. Establishment of appropriate check-in and check-out controls

Establishment of suitable, paperless and language-independent entry and exit controls for drivers and their transport containers, which enable the driver, the transport container and the company for which the driver works to be clearly identified, preferably digitally. For this purpose, all transport containers should be equipped with a global ITEM ID.

6. Setting up suitable identity checks

Appropriate controls of persons or their activities involved in loading, unloading or cleaning. This ensures that everyone completes their tasks without themselves facing the possibility of intentional contamination (microbial infestation, contamination, exposure to residues and possible foreign bodies, biological, chemical and physical hazards), tampering or sabotage, for example during loading, unloading or cleaning to have.

7. Cleaning of the transport containers according to defined cleaning standards

Uniform cleaning and disinfection plans or cleaning programs/ -procedures (for example ENFIT cleaning standards) are to be maintained and applied in a correspondingly verifiable manner. Evidence of the effectiveness of cleaning and disinfection (validation, verification) must be provided regularly. After the cleaning and disinfection has been carried out, it must be ensured that hygienically perfect drying takes place.

8. Security Measures for Transport

Ensuring that transport containers between all stations, from the cleaning station to loading, loading to unloading and unloading to cleaning, are closed, secured with seals and tested in accordance with DIN 10 502-1.

9. Definition of the transfer of risk

Ensuring that the correct number of required seals are not affixed by the driver after cleaning, but by the staff at the cleaning station (passing of risk). It is common practice for drivers to order a certain number of seals when placing the order for cleaning, without the cleaning station controlling or being able to control how many seals are required for a specific transport container. (Missing information on the number and positions of seals).
To save time and money, drivers attach the seals themselves. This gives drivers the possibility of manipulation themselves, e.g. by bringing in dirt. In practice, it is not uncommon for some drivers to attach the seals much later, after cleaning. For example when taking a

break or just before the next load. During this time it is easy for third parties to manipulate or sabotage.

10. Establishment of container testing centers and use of tested transport containers

Construction of container testing centers, according to DIN 10 502-1, with trained experts who are able to identify the critical points, their number and position of a transport container (manholes, pipelines and screw connections, hose boxes, filters, overflow and vacuum valves, pumps, etc.). They are able to install effective and standardized protective devices that are secured against manipulation or sabotage with appropriate seals.

Ideally, this information should be digitally accessible to all participants involved in the application and testing of seals. The information includes a seal plan, the number and position of the items to be sealed, as well as the unique identification of the transport container with a global digital ITEM ID (Global Transport Container Identification), so that the manipulation-free security suitable seals can be clearly assigned to the transport container. Exclusive use of tested transport containers.

11. Use of digital seals with a unique QR code

Development of an international standard for tamper-free and non-overlapping, digitally usable seals with a unique QR code (seal ID), which is clearly assigned to the transport container or its ITEM ID by scanning it with a smartphone or tablet. The data transmission should take place via a suitable cloud platform to the recipient of the transport container, so that the recipient can first digitally and error-free check the integrity of the seals and their assignment.

12. Recruitment criteria for critical infrastructure personnel

Development of standards for producers, logistics and transport companies, cleaning stations, warehouses and depots, inspection bodies and container testing centers that ensure that only trustworthy, sensitized and trained personnel work in sensitive areas.

13. Application and control of security measures

Development of standards on how, where and by whom seals are to be attached, or how, where and by whom seals are checked for integrity, completeness and clear assignment to the transport container. These people must also be able to reliably identify tampering or sabotage. Findings must be documented and forwarded in order to be able to initiate appropriate measures.

14. Further and further training of the official control staff

Uniform training and further education and sensitization of the official control staff on the aforementioned topics.

Hans-Dieter Philipowski
ENFIT - President

Maik Maschke
BVLK - President

2022-11-30 Brüssels